APPLICATION OF CRYPTOGRAPHY FOR INFORMATION SECURITY IN UMARU MUSA YAR'ADUA UNIVERSITY, KATSINA

BY

Abdulrashid ABUBAKAR

Department of Library and Information Science
Faculty of Education
Ahmadu Bello University, Zaria

November, 2014

APPLICATION OF CRYPTOGRAPHY FOR INFORMATION SECURITY IN UMARU MUSA YAR'ADUA UNIVERSITY, KATSINA

BY

Abdulrashid ABUBAKAR
MSC/EDUC/151/2011-2012

A Thesis Submitted to the School of Postgraduate Studies
Ahmadu Bello University, Zaria

In Partial Fulfillment of the Requirements
for the Award of Masters Degree in Information Science

Department of Library and Information Science
Faculty of Education
Ahmadu Bello University, Zaria

November, 2014

DECLARATION

I hereby declare that this thesis entitled "Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina" has been carried out by me under the supervision of Professor Zakari Mohammed and Dr. Ezra Shiloba Gbaje. The Information derived from the literature has been duly acknowledged in the text and list of references provided. No part of this work has been previously presented for the award of another degree or diploma at this or any other institution.

Abdulrashid Abubakar

---------- ----------

Signature Date

CERTIFICATION

This thesis entitled "Application of Cryptography in Information Security in Umaru Musa Yar'adua University, Katsina" by Abdulrashid Abubakar has met the requirements governing the award of the degree of Master in Information Science of Ahmadu Bello University, Zaria and is approved for its contribution to knowledge and literary presentation.

_____ _____

Prof. Zakari Mohammed Date
Chairman, Supervisory Committee

_____ _____

Dr. Ezra Shiloba Gbaje Date
Member, Supervisory Committee

_____ _____

Dr. Abdullahi Musa Ibrahim Date
Head of Department

_____ _____

Date

Prof. A. Z. Hassan
Dean, Postgraduate School

DEDICATION

This work is dedicated to my parents, Alhaji Abu Ali Abubakar Rafindadi and Hajia Ummulkhair Rafindadi.

ACKNOWLEDGEMENT

First and foremost, I will like to register my appreciation to Almighty Allah, the Most Gracious, Most Merciful, and the Sustainer of the universe who bestowed all means and favour to me to successfully complete this project work.

My profound gratitude goes to my Supervisor, Professor Zakari Mohammed for his encouragement, constructive criticism, understanding and patience throughout the period of this work despite his tight schedules**.** I also acknowledge with appreciation, the contributions of my Co-supervisor Dr. Ezra Shiloba Gbaje who also devoted substantial part of his time to offer useful suggestions, constructive criticism, guidance and re-shaped the work at various stages. My sincere gratitude and appreciation go to the Dean Faculty of Education, Prof. Tijjani Abubakar; the Head of the Department of Library and Information Science, Dr. Abdullahi Musa Ibrahim. I say a big thank you for your love, concern and encouragement.

I would like to warmly thank my lecturers in the Department of Library and Information Science, Ahmadu Bello University Zaria for their support, particularly Dr. Babangida Umar Dangani, Dr. Kosoko Adu Momoh, Dr. Baba Aduku, Dr. Abu Yusufu, Mal. Hayatu M. Musa, Mrs. M.F. Mohammed, Mal. Idris A. Dauda and Mal. Jibrin Abdurrahman for their moral and constructive criticisms and willingness to help at all times. I say thank you for your encouragement and support.

I am very much thankful to the Head, Management Information System and the entire Directorate of Information and Communication Technology staff of UMYUK, for their contributions towards this work by providing me with the necessary information. I also wish to thank Dr. M.O Ibrahim and Dr. Lawal

Umar for persistently encouraging me to hurriedly complete this research work. Their words of encouragement are highly appreciated.

Finally, I wish to also express my deep gratitude to my mother and father who inspired me to be steadfast. I am obliged to thank my brothers and sisters for their patience and understanding while undertaking this course of study. May God in His infinite mercy and abundant blessings bless everybody that assisted me in one way or the other.

TABLE OF CONTENTS

CHAPTER FOUR: DATA PRESENTATION, ANALYSIS AND DISCUSSION

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	-	Automated Teller Machine
CD	-	Compact Disk
DBA	-	Database Administrator
DBMS	-	Database Management System
DDL	-	Database Domain Language
DDOS	-	Distributed Denial-of-Service
DF	-	Degree of Freedom
DICT	-	Directorate of Information and Communication Technology
DOS	-	Denial of Service
DVD	-	Digital Video Disk
IACR	-	International Association for Cryptologic Research
ICT	-	Information and Communication Technology
IDS	-	Intrusion Detection Systems
IT	-	Information Technology
JIT	-	Just-In-Time
HTML	-	Hypertext Markup Language
MD5	-	Message Digest-5
MSN	-	Microsoft Network
OLAP	-	On-line Analytical Processes
OLTP	-	On-line Transaction Processing
OODBMS	-	Object-Oriented Database Management System
OS	-	Operating System
PKC	-	Public-Key Cryptography

PPMC	-	Pearson Product Moment Correlation
RATs	-	Remote Access Tools
RDBMS	-	Relational Database Management System
SHA-1	-	Secure Hash Algorithm-1
SHA-224	-	Secure Hash Algorithm-224
SHA-256	-	Secure Hash Algorithm-256
SHA-384	-	Secure Hash Algorithm-384
SHA-512	-	Secure Hash Algorithm-512
SSL	-	Secured Shell
SQL	-	Structured Query Language
UMYUK	-	Umaru Musa Yar'adua University, Katsina.
URL	-	Universal Remote Locator
XQUERY	-	Extended Query
XXS	-	Cross Site Scripting

ABSTRACT

This study sets to investigate the Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina. Four research questions were formulated and two hypotheses tested at α 0.05. The research questions, among others, sought to find out what types of databases are available and accessible in Umaru Musa Yar'adua University, Katsina? What types of security threats are databases in Umaru Musa Yar'adua University, Katsina exposed to? Survey research design was used for this study. The population of the study comprised all staff of the Directorate of Information and Communication Technology in Umaru Musa Yar'adua University, Katsina. Due to the fact that the population is not too large, all the 21 staff were used as sample for this study. Hence no sampling technique was applied. Questionnaire and observation were the instruments used to collect data for this study. The data collected were presented and analysed using frequency distribution tables, and percentages. While null hypothesis one was tested using PPMC and null hypothesis two was tested using Chi-Square. The study found among others that personnel records database, financial records database, transcript records database, and student academic records database were the types of databases available with the highest frequencies of 100.0% response scores respectively in UMYUK. It was also revealed that data tempering, password-related threats, worms, intrusion by unauthorized users, clicking unnecessary links and privilege abuse were the security threats exposed to the databases with the highest frequencies of over 60% response scores respectively in the University. On the hypotheses tested, it was found that there is no significant relationship between database accessibility and the types of security threats they are exposed to in Umaru Musa Yar'adua University, Katsina. Application of cryptography has no significant effect on the prevention of security breaches of databases in the University studied. This study recommended that the University should adopt strategic information records database for keeping records of valuable assets, day-to-day operations, and executive decision-making and intellectual rights in efforts to prevent theft of institutions' secrets and confidential documents. Lastly, Information security risk assessment and management should be made an integral component of DICT policy document. This would go a long way in preventing and minimizing the threat level of data by intruders and other malicious attacks in the University's databases. This is a prerequisite for the University to successfully survive and compete in the 21st Century.

.

CHAPTER ONE

INTRODUCTION `

1.1 Background to the Study

The 21ST Century is designated the information age, because of the crucial role of information in its evolution. According to Sveiby (1994), the word information is derived from Latin “informare” which means give form to. Most people tend to think of information as disjointed little bundles of "facts". Due to the dynamic nature and ever changing characteristic tendencies of information, Mohammed (2012) conceptualized information as whatever we physically or otherwise come across consciously or unconsciously, accidentally or intentionally and regularly or occasionally that adds positively or otherwise to our existing knowledge; education and training; curricula; skills; practices; ideas; ideals; culture; tradition; belief; expectations; experiences and wellbeing.

The mode and presentation of information is enhanced by the use of appropriate Information and Communication Technology (ICT). ICT can simply be referred to as an information system comprised of organized information manager and users; computer hardware and software; communication networks and data/information resources that acquire and collect, organize and transform; store and receive; as well as disseminate and transfer relevant information to the relevant users, regardless of their location, time of accesses and need, and irrespective of their strata in society (Mohammed, 2009).

One of the main paradigm shifts of the emerging information society is that information is becoming a crucial if not the most important resource (Maurer, 2004). Information is currently created, stored, preserved and transmitted in

electronic format. Electronic information is the lifeblood of many organizations and consequently needs to be suitably protected. This is especially important in an increasingly interconnected academic environment where information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Even though advancement in Information Technology (IT) has enhanced universal electronic connectivity which poses new challenges to security, such as social engineering, phishing, viruses, hacking, electronic eavesdropping and electronic fraud, there is no time at which information security does not matter. Cyber criminals are clever, innovative, well financed, and technically proficient and are willing to take extraordinary efforts to attack information system. In order to combat them, there is the need to be familiar with their tactics and techniques, learn how to safeguard the information, and follow the best practices with respect to information security. Achieving information security in an academic environment requires a vast array of technical and legal skills. The technical means to deal with information insecurity particularly information stored in a database is provided through cryptography.

However, for electronic databases to be secured against security breaches and threats, an understanding of issues related to cryptographic techniques in general is necessary. The popularization of the Internet has brought fundamental changes to the world, because it allows a universal method of communication between computers. This carries enormous benefits with it, but also raises many security considerations.

Safety and Security Centre (2014) posited that phishing email messages, websites, and phone calls are designed to steal money and sensitive information.

Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer. They also use web addresses that resemble the names of well-known companies or organizations but are slightly altered. They might email you, call you on the phone, or convince you to download something off of a website. In order to access a fake site the user has to enter their credentials. This information is exactly what the phishers are after. Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. Granger (2001) remarked that Social Engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system. Menezes *et al* (1997) assert that "security is necessary when communicating multimedia data over any un-trusted medium such as public networks, and in particular, the Internet in order to protect information from theft, alteration or misuse". Cryptography is a fundamental technology used to provide security of computer networks; it also provides means of detection and remediation of security breach and vulnerabilities (Savu, 2013).

1.1.1 Cryptography

Cryptography comes from two Greek words 'Kryptos' and 'Graphein', which mean hidden and writing, respectively (Pawlan, 1998). The term cryptography is referred to as the change of data representation from its original form into another different form in order to make it hidden and secured. Cryptography has two processes; the first process is the encryption where the original data is converted into secured form using certain steps. The second process

is the decryption, where the encrypted data is restored to the original form by applying the inverse steps applied in the encryption process (Issam, 2010). Cryptography is the practice of hiding information so that unauthorized persons cannot read it. The literal meaning of cryptography is "hidden writing": how to make what you write obscure, unintelligible to everyone except whom you want to (Savu, 2013).

It is believed that classic cryptography started thousands of years ago. All over the history, classic cryptography was used for secret communications between people. This kind of cryptography is usually applied by substituting the message letters by other letters using certain formula. For example substituting each letter in a message with the next letter in the alphabets so that the word "Test" would become "Uftu" (Issam, 2010). Modern cryptography, however, is not limited only to maintaining the secrecy of information but also to: ensuring the identity of the communicating parties (authentication); ensuring that information is not tampered by others (integrity); and preventing any of the communicating parties from denying any received or sent information (non-repudiation) (White, 2003; Harris, 2007). Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication (Menezes, *et al.*, 1997).

Similarly, in modern cryptography, there are three types of cryptographic schemes: secret key (symmetric) cryptography, public-key (asymmetric) cryptography, and hash functions. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. This was the only type of encryption technique publicly known until 1976. Whitfield and

Hellman in 1976, proposed the notion of public key cryptography, which was also known as asymmetric key cryptography. It uses two keys, one for encrypting information by the sender, and other one for decrypting information by the receiver. The hash function, also called message digest or one-way encryption, is a transformation that takes an input and returns a fixed-sized string, which is called the hash value. While symmetric or asymmetric encryption methods provide the means to ensure information confidentiality, hash functions provide a measure of the integrity of a file. For instance, hash algorithms are typically used to provide a digital signature of a file's contents and to ensure that the file has not been altered by an intruder or virus (White, 2003; Harris, 2007).

Cryptography, the art and science of hiding data, plays a central role in achieving information security. Cryptography has become a fundamental part of communication and commercial applications on the Internet as well as in many other digital applications. Cryptography is deployed with cryptographic algorithms, mathematical functions for hiding messages and retrieving hidden messages (Jarvinen, 2008).

1.1.2 Historical Background of Umaru Musa Yar'adua University, Katsina

Umaru Musa Yar'adua University (UMYU), formerly Katsina State University was established by the Katsina State Government out of the desire to improve access to higher education for its citizenry. The law establishing the Katsina State University was passed by the Katsina State House of Assembly on 5th September, 2006. The University commenced academic activities in January, 2007 with three Faculties (Education, Humanities & Natural and

Applied Sciences), and 16 undergraduate programmes. The University will build upon existing academic strength, a total of 13 Faculties, 76 Departments and 236 academic programmes (undergraduate and postgraduate) at the end of its 25 year period of its academic phasing, which is divided into four years each.

1.1.3 Information System

Information System is complementary networks of hardware and software that people and organizations use to collect, filter, and process, create, and distribute data (Jessup, Leonard, Joseph and Valacich, 2008). Information Systems inter-relate with database systems on the one hand and activity systems on the other. It is a form of communication system in which data represent and are processed as a form of social memory. It can also be considered as semi-formal language which supports human decision making and action. It is the primary focus of study for organizational informatics (Basden, 2010). John and Joe (2002) argue for advantages of viewing an information system as a special type of work system. A work system is a system in which humans and/or machines perform work (processes and activities) using resources to produce specific products and/or services for customers. An information system is a work system whose activities are devoted to processing (capturing, transmitting, storing, retrieving, manipulating and displaying) information.

Similarly, Kioskea (2013) posited that information system is any electronic system that stores, processes or transmits information. Typical information systems include data about people, software, hardware such as workstation, servers, smart

boards, mobile devices e.g. smart phones, network devices like firewalls, routers and procedures among others. Organizations are increasingly relying on these distributed systems to gain productivity and efficiency advantages. Database systems are an integral component of these information systems and hold all the data which enables the whole system to work. Most organizations such as tertiary institutions and firms spend large amount of money these days in order to achieve the best security standards for the database systems.

1.1.4 Database System

A database consists of organized pieces of information. These pieces of information are placed into records. Database system is considered as a collection of related data. Database Management System (DBMS) is a software that manages (define, create and maintain) and controls the access to the database, and a collection of database application(s) a program that interacts with the database at some point in its execution (typical example is SQL statement) along with the DBMS and the database itself (United Kingdom Essays, 2013).

The database is an obvious place where data accumulate and is potentially accessible to range of information systems and users. In most tertiary institutions, databases can be treasure troves of sensitive information. They can contain staff data, students' data, personal data, confidential competitive information, and intellectual property to mention a few. Lost or stolen data, especially students' data, can result in damage and competitive disadvantage.

Secure and secret means of communication has been always desired for organization especially in the field of database systems. There is always a possibility of interception by a party outside of the sender-receiver domain when

data is transmitted. Modern digital-based encryption methods form the basis of today's world database security. Encryption in its earlier days was used by military and government organizations to facilitate secret information but in present times it is used for protecting information within many kinds of civilian systems. In 2007, the U.S. Government reported that 71% of companies surveyed utilized encryption to some of their data in transit (Richardson, 2008).

Database security requires knowledge of both database management and security. Securing the database may be the single biggest action an organization can take to protect its assets. Data is a valuable resource especially in an academic environment; therefore they have a very strong need of strictly controlling and management. It is the responsibility of the DBMS of the organization to make sure that the data is kept secured and confidential as it is the element which controls the access to the database (Steve, 2007).

Most sensitive and proprietary data in universities reside in a DBMS such as admission records, student records, students results (transcripts), school fees, course registration among others, thus the security of the DBMS is a primary concern. This is with respect to both the internal and the external users. The internal users are the universities employees like database administrators, application developers, and end users who just use the application interface, which fetch its data from one of the databases and the external users can be the employees who do not have access to the database or an outsider who has nothing to do with the institution.

1.1.5 Challenges of Database System

Databases are the storage areas where large amount of information is stored. The nature of information stored varies and depends on different organizations and

companies. Nevertheless, every type of information needs some security to preserve data. The level of security depends on the nature of information. For example, the military databases require top and high level security so that the information is not accessed by an outsider but the concerned authority because the leakage of critical information in this case could be dangerous and even life threatening. Whereas the level of security needed for the database of a public server may not be as intensive as the military database (Kayarkar, 2012).

Most Nigerian tertiary institutions' databases hold sensitive and valuable data/information such as students' academic records (examination records, personal profile records, transcripts records, courses registration records) among others. Even though perimeter and network security measures create a barrier against some type of attacks; there are attack patterns that take advantage of database-specific vulnerabilities. SQL injection, buffer overflow attacks and other attacks can cut right through Web firewalls, application firewalls and Intrusion Detection Systems (IDS) and create opportunities for data theft, unauthorized modification or destruction of data, or breaches of privacy and personally identifiable information.

However, the database systems in most universities are affected by the following threats:

1. Unauthorized access and modifications of original work of some determined and erudite scholars from online library databases.
2. Changing or alteration of results.
3. Changing or alteration of personal data e.g. Date of birth, state of origin and marital status among others.

Sentrigo (2007) commented that Database Management Systems are complex, supporting an ever growing set of requirements and platforms, with addition of features they develop gaps in security vulnerabilities that are constantly being discovered by users, ethical hackers and unfortunately, non-ethical hackers as well. Such vulnerabilities are reported to DBMS vendors who do their best to patch them, but this is a process that currently takes several months on average, and in some cases years. That time lag is essentially an open invitation to exploit the vulnerability and breach the database in many organizations.

As the volume of information grows and continues to be increasingly stored and communicated electronically, it is therefore mandatory for organizations to take certain measures to ensure the security of their sensitive information.

1.1.6 Information Security

Information Security is such a broad discipline that it's easy to get lost in a single area and lose perspective (Miessler, 2013). Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms (Savu, 2013). The United States National Information Systems Security Glossary (2012) defines Information Systems Security as " protection of information systems against unauthorized access to or modification of information, whether in storage, process or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats". Schneider (2013) saw information

security as a means of protecting information and information systems from unauthorized access, use, disruption, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably.

Similarly, information security refers to the processes and methodologies involved in keeping information confidential, available, and assured of its integrity. Good information security means that one's personal data is protected against theft and misuse and that the data one needs to do his/her job will be available and accurate. Maintaining security will require one to take some precautions to protect oneself and the entire institution (Techopedia, 2011).

The evolution of computer networks has made the sharing of electronic information ever more prevalent in most Nigerian universities such as online admission, online courses registration, checking of result online and online payment of school fees. Information is now exchanged at the rate of trillions of bytes per millisecond, daily numbers that might extend beyond comprehension or available nomenclature. A proportion of that data is not intended for sharing beyond a limited group and much data is protected by management concerned. The other factors which have made data security more crucial in institutions are the recent rapid growth of the web based information systems and applications and the concept of mobile databases.

Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license. Once they have gained your trust, cybercriminals might ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable (Safety and

Security Center, 2014). Thus, to establish an information system security in any organization, classifying the types of information in the organization's database systems and the security needs associated with them is the first and important step. As databases are used in a multitude of ways, it is useful to have some of the primary functions characterized in order to understand the different security requirements.

Most of the organizations use multiple hardware solutions like routers and firewalls to ensure the security of confidential data. Such devices can protect data because they keep any external threat out of the network. But intruders developed numerous ways to attack organizations' networks and obtain necessary information. In case one of them will work and organization's first line of defense will be penetrated, data encryption will ensure secret data won't be viewed. The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems.

1.1.7 Use of Cryptography for Information Security

Organizations in general need to protect their data from adversary and control how the data should be distributed both within and outside the organizations' boundaries. Universities in Nigeria are steadily subscribing to web-based information systems to manage their staff and students' information technically called portals. Portals technology are being designed, built and deployed by institutions to leverage on the many advantages of computerization to manage their information system. Information System security can be improved upon for such web-based system in order to protect and manage the institution and its confidential information by introducing cryptography. Savu (2013) opined that

cryptography can be applied to enhance access controls of data by preventing unauthorized personnel from entering or accessing the information systems and protecting information no matter where that information is, i.e. in transit or in a storage area.

Organizations are becoming more interconnected to open networks and other emergent global networks. The openness of these networks enables malicious cyber-attacks against sensitive organizations' assets and increases the potential risk to sensitive information. This risk is compounded through the use of the Internet and other non-secure mediums such as Wireless Local Area Network technology. This technology includes utilizing Laptops and Personal Electronic Devices (such as cellular telephones, pagers and hand held computers) to communicate and process information from any location. Hackers also use social engineering and phishing to deceive users and obtain sensitive information in a malicious way. An outside hacker use psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system. For example, a password from a person rather than breaking into a system. In reality, social engineering can be any and all of these things, depending upon where you sit (Granger, 2001).

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Websites. Websites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. A phishing expedition, like the fishing expedition it is named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishers use

a number of different social engineering and e-mail spoofing ploys to try to trick their victims (Rouse, 2007).

Encryption methods can protect sensitive information during storage and transmission. They provide important functionality to reduce the risk of intentional and accidental compromise and alteration of data. Encryption algorithms use a mechanism called a key, which is used to render the information unreadable during transmission. While the information is encrypted it is mathematically protected against disclosure because it cannot be read by someone who does not have a corresponding key to decrypt the information. Encryption methods serve as part of defense-in-depth strategy and provide reasonable protection of sensitive information in many organizations (National Academy of Sciences, 2013).

As demands for secured communication bandwidth grow, efficient cryptographic processing will become increasingly vital to good system performance. To introduce cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Regardless of who is involved, to one degree or another, all parties to a transaction must have confidence that certain objectives associated with information security have been met (Menezes, *et al.,* 1997).

From e-mail to cellular communications, from secure web access to digital cash, cryptography is an essential part of today's information systems. Cryptography has enabled the first secure transmission which has helped fuel the growth of transactions in many organizations like e-payment over the world’s biggest public network, the internet. Cryptography helps provide accountability, fairness,

accuracy, and confidentiality. It can prevent fraud in electronic commerce and assure the validity of financial transactions. It can protect your anonymity or prove your identity. It can keep vandals from altering your web page and prevent industrial competitors from reading your confidential documents. In the information dependent world we live today, cryptography can be found all around us, often in places where you would not expect it (Schneier, 1997). Internet applications such as, databases, and browsers store a tremendous amount of sensitive data, but frequently the data is left unprotected. The only way to make data secured in any application that runs over the internet is to use cryptography (Galbreath, 2003). Cryptography concerns itself with the following four information security objectives: Confidentiality, Integrity, Non-repudiation and Authentication (Lisa, 2009).

1.2 Statement of the Problem

The success of any organization depends on how secured the data stored in their databases is. In academic environments, databases contain personal profile, academic information about students are usually classified as sensitive. Often, the identity of an individual is stored in the database whether by name, personal code or a combination of attributes (Bagdanov, 2007). Databases and their applications form one of the most important classes of computer systems yet they have received relatively little attention from many organizations (Elsevier, 2014).

Most tertiary institutions embrace the use of web applications and migrate more of their critical functions to the internet such as online admission, online registration and online checking of results to mention a few. As such, intruders could have more opportunity and incentive to gain access to institutions' sensitive

information through these web applications. Hackers target web applications because they easily provide access to the most valuable records in the insitutions such as personal profile records, employment records, medical records, accommodation records, admission records and students' academic records (examinations records, transcript records, courses registration records) as well as other sensitive information. While most websites are heavily secured at the network level with firewalls, these sites still allow intruders complete access to the institutions through web application manipulation. Intruders can hack into the web applications by identifying how the application is intended to work and finding backdoors that could be used to access these applications.

It has been established that Nigeria is an impressionable country (Ibikunle, 2013). However, it seems some, if not all, of Nigerian Universities websites are in danger. The official website of Ahmadu Bello Univeristy, Zaria (www.abu.edu.ng) has been hacked during the 2014/2015 academic session. Those that wrote A.B.U, Zaria, Post UTME 2014 faced difficulty in checking their results when the University website was hacked (Nairaland , 2014). According to Binjo (2012), Hackers got into the official website of the University Of Lagos at http://unilag.edu.ng and replaced the website with pornographic pictures.

Hackers attack Universities' websites for various reasons: for money, to obtain knowledge or intellectual property, institutions sabotage, for fun or because they can. According to NGScholars (2014), the official website of Bayero University, Kano, www.buk.edu.ng has been hacked by members of the "Nigerian Cyber Army". According to a message posted by the group, they are protesting the current ASUU strike which has lasted for over 100 days.

If the security attached to these systems is vulnerable, cyber-criminals could interfere with the databases and manipulate the systems without a trace. Such protection is needed to preserve the privacy of an individual in the institution and prevent abuse of the data stored. Christian Kirsch-Thales (2009) posited that "the shortcomings of many traditional database security techniques such as firewalls and application security have been exposed in recent years and it is now broadly recognized that these approaches to database security are no longer sufficient to protect data in today's modern, open and complex IT environment. In trying to mitigate the risk of security breaches to electronic databases, cryptography is often seen as the solution". Cryptography is one of the techniques that will be able to ensure more privacy and authenticity in transmission of information electronically.

In Umaru Musa Yar'adua University, Katsina, students' academic records are usually stored in the database (web based). Each time a Lecturer conducts a test or examination, he posts the result via the web based system to the Departmental Level Coordinator who in turn sends the information to the Examinations Officer through the same system for further moderation by examinations committee. There are several security measures put in place to safeguard the institutions' data. These include but not limited to protection against SQL injection, data encryption , brute force attack and database redundancy. All these measures, though highly efficient in safeguarding any web based data, still leave the institutions data vulnerable to phishing scams, social engineering, spyware, malware and intruders. External security system involves the process of authenticating web data from unauthorized access but using phishing scams, social engineering and spyware, unauthorized users could gain access to staff or student login details hence can access, modify

and process such data without a mandate from the University authorities concerned. Many tertiary institutions face the challenges of implementing protection and information security measures to meet a wide range of requirements that lie beyond regulatory compliance. This is a big challenge that becomes an imperative for this study.

1.3 Research Questions

The study sought to provide answers to the following research questions:

1. What types of databases are available and accessible in Umaru Musa Yar'adua University, Katsina?
2. What types of security threats are databases in Umaru Musa Yar'adua University, Katsina exposed to?
3. To what extent has cryptography prevented the security breach of databases in Umaru Musa Yar'adua University, Katsina?
4. What are the challenges encountered in the application of cryptography in Umaru Musa Yar'adua University, Katsina?

1.4 Research Hypotheses

This study was designed to test the following hypotheses:

H_1: There is no significant relationship between database accessibility and the types of security threats they are exposed to in Umaru Musa Yar'adua University, Katsina.

H_2: Application of cryptography has no significant effect on the prevention of security breach of databases in Umaru Musa Yar'adua University, Katsina.

1.5 Objectives of the Study

The general objective of the study was to investigate the Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina. The specific objectives of this study are:

1. To identify the types of databases available and accessible in Umaru Musa Yar'adua University, Katsina.
2. To identify the types of security threats that databases in Umaru Musa Yar'adua University, Katsina are exposed to.
3. To examine the extent to which cryptography has prevented the security breach of databases in Umaru Musa Yar'adua University, Katsina.
4. To identify the challenges encountered in the application of cryptography in Umaru Musa Yar'adua University, Katsina.

1.6 Significance of the Study

This research "Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina" when completed would serve as policy document for security of database system in UMYUK. It would also help the Management of Umaru Musa Yar'adua University, Katsina and Directorate of Information and Communication Technology to appreciate the relevance of Cryptography to the security of e-resources.

Likewise, the findings of this research work would hopefully benefit Katsina State in particular and Nigeria at large in the area of information security as part of defense-in-depth strategy for providing reasonable protection of vital information vis-à-vis the means of detection and remediation of database security breaches against well meaning insiders, targeted attacks and malicious insiders.

Finally, the research would provide an empirical evidences that would expand the frontier in the area of cryptography and would serve as a useful guide to the would be researchers interested in this special area of research.

1.7 Delimitations of the Study

The scope of this research work covered most of the databases in Umaru Musa Yar'adua University, Katsina which include: personnel records database, financial records database, student hostel records database, student academic records database and medical records database. While registry records database, library records database and physical planning records database are excluded in the scope of the study.

1.8 Limitations of the Study

This study was limited to the Application of Cryptography for Information Security in UMYUK due to some constraints which include the inability of the researcher to get access to some relevant documents and information for this study as well as time within which to complete the project. Also the target respondents were the Directorate of Information and Communication Technology Staff of the UMYUK.

1.9 Operational Definition of Key Terms

The following terms were defined operationally as used in this study:

Cryptography: The word cryptography is the change of data representation from its original form into another different form in order to make it hidden and secured. In modern cryptography, there are three types of cryptographic schemes: secret key (symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions.

Decryption: This process is called as “Decoding the message” or “Decrypting the Message”. This process basically reverses the effects of the encryption process on the message.

Encryption: Is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.

Information: Is a collection of data that have been interpreted and examined for patterns and structure.

Information Security: Is a protection of confidential information against threats to its integrity or inadvertent disclosure.

References

Bagdanov, D. (2007). How to Securely Perform Computation on Secret Shared Data. Unpublished MSc. Thesis: University of Tartu.

Binjo (2012). Cyber-Crime, Education. Retrieved on 2nd November, 2014 from http:// www.technsstivity.com/category/education/

Basden, A. (2010). On Using Spheres of Meaning to Define and Dignify the IS Discipline. *International Journal of Information Management*, 30, 13-20.

Christian Kirsch –Thales (2009). The Role of Encryption in Database Security. Retrieved 14th January, 2014 from http://www.net-security.org/insecure-archive.php.

Elsevier, B.V. (2014). Database systems: challenges and opportunities for graphical HCI. Retrieved April, 2014. From http://www/.elsvier.com/.

Galbreath, N. (2003). Cryptography for Internet and Database Applications: Developing Secret and Public Key Techniques with Java, Retrieved 15h January, 2014 from http://eu.wiley.com/WileyCDA/Section/id-302479.html?query=Nick+Galbreath.

Granger (2001). Social Engineering Fundamental, part 1: Hacker tactics.

Harris, S. (2007). CISSP® All-in-One Exam Guide. McGraw-Hill.

Ibikunle, F. (2013). *Approach to Cyber Security Issues In Nigeria*. Retrieved 2nd November, 2014, from *http://ijcrsee.com/index.php/ijcrsee/article/view/11/114*

Issam, M. (2010). Efficient Hardware Implementations for the Advanced Encryption Standard (AES) Algorithm. Unpublished MSc. Thesis Dalhousie University Halifax, Nova Scotia.

Jarvinen, K. (2008). Studies on Efficient Implementation of Cryptographic Algorithms. Unpublished PhD. Dissertation Helsinki University of Technology.

Jessup, Leonard M. Joseph S. Valacich (2008). *Information Systems Today* (3rd ed.). Pearson Publishing. Glossary p. 416.

John, W., and Joe, P. (2002). Strategic Planning for Information System. 3rd Ed. West Sussex. John Wiley & Sons Lt

Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. M.G.M's College of Engineering and Technology, Navi Mumbai, India

Kioskea (2013). Introduction to Information Technology Security. Retrieved on May, 2013. From http://www.facebook.com/pages/Kioskea/117422445065179.

Lisa, W. (2009). Fast Flexible Architectures for Secure Communication. Unpublished MSc. Thesis, University of Michigan.

Maurer, U. (2004). The Role of Cryptography in Database Security. Zurich, Switzerland: Springer.

Menezes, A.J. Van Oorschot, P.C. And Vanstone, S.A. (1997). *Handbook of Applied Cryptography*. London: CRC Press.

Miessler, D. (2013). An Information Security Concepts Primer. Retrieved on 9th May, 2013. From http//creativecommon.org.

Mohammed, Z. (2009). Capacity Building for Library and Information Centre Personnel in ICT Environment. Ahmadu Bello University, Zaria. *Pp.9-13.*

Mohammed, Z. (2012). Fifty Years of Library and Information Service in Ahmadu Bello University, Zaria. *A Paper Presented at the Symposium to Mark the Ahmadu Bello University, Zaria 50th Anniversary Golden Jubilee Celebrations.*

National Academy of Sciences (2013). Cryptography's Role in Securing Information Society. Retrieved 24, May, 2013 from http://www.nasonline.org/about-nas/150th-anniversary/

Nairaland (2014). A.B.U Zaria 2014/2015 Admission Thread – Education. Retrieved 2nd November, 2014 from *www.nairaland.com/1582985/a.b.u-zaria-2014-2015-admission/40*

NGScholars (2014). ASUU Strike: Bayero University Website Hacked. Retrieved 2nd November, 2014 from http: // *www.ngscholars.com*/category/

Pawlan, M. (1998). Cryptography: The Ancient Art of Secret Messages. Retrieved May 4, 2013, from http://www.pawlan.com/Monica/crypto/

Richardson, R. (2008). CSI Computer Crime and Security Survey. California: Irvine.

Rouse. M (2007). Definition of Phishing. Retrieved on 15th April, 2014. From http://searchsecurity.techtarget.com/definition/phishing

Safety and Security Centre (2014). How to Recognize Phishing Email Messages, Links, or Phone Calls. Retrieved on 15th April, 2014. From http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx.

Savu, L. (2013). *Cryptography Role in Information Security.* Ramonia University of Bucharest, Romania.

Schneider, L. (2013). Information Security - Learn about Information Security. Retrieved on 18th April, 2013 from *http://www.about.com/*.

Schneier, B. (1997). Cryptography, Security and the Future. Retrieved 10th April, 2014. From http://www/schnnier.com/cryptography.html.

Sentrigo (2007). Whitepaper, the Need for Real-Time Database Monitoring, Auditing and Intrusion Prevention. RADirect Inc Corporate 900 Drive Mahwah.

Steve, G. (2007). Databases for Embedded Systems. *Embedded Computing Design* magazine. Retrieved on August 13, 2013 from http//www.embedded-computing.com.

Sveiby, K.E (1994). *What is Information*. Retrieved 12th April, 2014. From http://www.sveiby.com/articles/polanyi.html

Techopedia (2011). *The Seven Basic Principle of IT Security* Retrieved 7th, May, 2013 from http// www.techopedia.com

Umaru Musa Yar'adua University, Katsina Official Website: http://www.umyu.edu.ng (n.d.)

United Kingdom Essays (2013), Database security and encryption retrieved 5th July, http://www.ukessays.com/

United State National Information Systems Security Glossary (2012). Definition of Information Security. Las Vegas, University of Nevada. Retrieved on 18th April, 2013 from *http://oit.unlv.edu/network-and-security*.

White, B. (2003). Cisco Security+ Certification: Exam Guide. McGraw-Hill.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1 Introduction

This chapter reviewed relevant literature related to the study based on the following sub-headings:

2.7 Application of Cryptography for Information Security.

2.8 Types of Databases Available and Accessible.

2.9 Security Threats Faced by Databases

2.10 Cryptography Prevention of Security Breach.

2.11 Challenges Encountered in the Application of Cryptography.

2.12 Summary of the Review.

2.2 Application of Cryptography for Information Security

In organizations where virtually all data of any importance is held on a computer system the necessity of cryptography cannot be disputed. In tertiary institution for example, this includes information on students such as examination records, admission, course registration and personal profile information among others. Cryptography can be used to provide message confidentiality and integrity and sender verification.

When people started doing business online and needed to transfer funds electronically, the applications of cryptography for integrity began to surpass its use for secrecy. Hundreds of thousands of people interact electronically every day, whether it is through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The constant increase of information

transmitted electronically has lead to an increased reliance on cryptography and authentication.

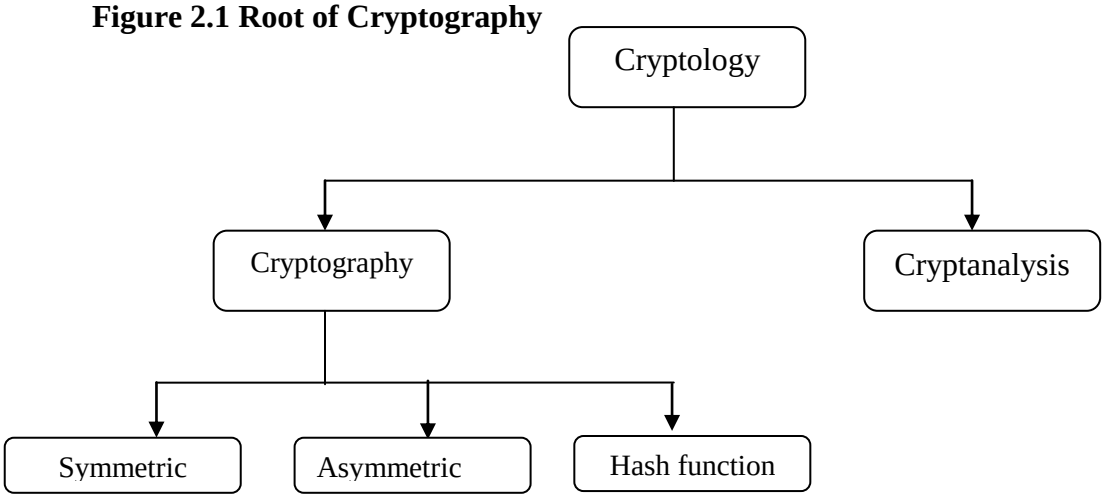
Cryptography is the art of combining some input data, called the plaintext, with a user-specified password to generate an encrypted output, called ciphertext, in such a way that, given the ciphertext, it is extremely difficult to recover the original plaintext without the encryption password in a reasonable amount of time (Kremlin, 2008).

Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. Cryptography allows people to carry over the confidence found in the physical world to the electronic world. It allows people to do business electronically without worries of deceit and deception. In the distant past, cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the message and authenticity of the sender *(*Pawliw, 2009*).*

Paar and Pelzl (2010) posited that the most general term is cryptology and not cryptography. Cryptology splits into two main branches: Cryptography and Cryptanalysis. Where Cryptography is the science of secret writing with the goal of hiding the meaning of a message; and Cryptanalysis is the science and sometimes art of breaking cryptosystems. One might think that code breaking is for the intelligence community or perhaps organized crime, and should not be included in a

serious classification of a scientific discipline. However, most cryptanalysis is done by respectable researchers in academia nowadays.

Figure 2.1 Root of Cryptography



Source: (Paar and Pelzl, 2010)

Cryptography is the art of "extreme information security." It is extreme in the sense that once treated with a cryptographic algorithm; a message (or a database field) is expected to remain secure even if the adversary has full access to the treated message. The adversary may even know which algorithm was used. If the cryptography is good, the message will remain secure. This is in contrast to most information security techniques, which are designed to keep adversaries away from the information. Most security mechanisms prevent access and often have complicated procedures to allow access to only authorized users. Cryptography assumes that the adversary has full access to the message and still provides unbroken security. That is extreme security. A more popular conception of cryptography characterizes it as the science of "scrambling" data. Cryptographers invent algorithms that take input data, called plaintext, and produce scrambled output. Scrambling, used in this sense, is much more than just moving letters around or exchanging some letters for others. After a proper cryptographic scrambling, the

output is typically indistinguishable from a random string of data. For instance, a cryptographic function might turn "Hello world!" into 0x397B3AF517B6892C (Kenan, 2005). The constant increase of information transmitted electronically was led to an increased dependence on cryptography in many organizations. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit either electronically or physically and while information is in storage (Savu, 2013).

Cryptography, the art and science of keeping messages secure, has a long fascinating history. During and before World War II, the main applications of cryptography were military. Both coding theory and cryptography originated with the seminal work of Claude Shannon in 1948. With the spread of computers and electronic communications after the war, the use of cryptographic schemes for passwords, banking transactions and various aspects of computer security proliferated. So did the uses of error-correcting codes in radio based communication systems and satellite communications. These uses and the evolving theory of codes generated much mathematical activity (Pell, 2013).

The earliest forms of cryptography are traced in the cradle of civilization, which comes as no surprise, including the regions currently encompassed by Egypt, Greece and Rome. As early as 1900 B.C., Egyptian scribes used hieroglyphs in a non-standard fashion, presumably to hide the meaning from those who did not know the meaning (Whitman and Mattord, 2005).

The Roman method of cryptography was known as the Caesar Shift Cipher; it is said that the great Roman Emperor Julius Caesar sent coded messages to his Generals on the front during the battles because he did not trust anyone, not even his

own messengers. It is said that he used a very simple coding system to do his job. He used to substitute every A in his letter with a D, every B with an E and so on. This is today commonly known as the "Shift by Three Rule". So, as only he and his Generals knew this rule, his messages remained highly secure and no one intruded them (Taylor, 2002).

As for the Greek method of using a stick, once the method was known, it was a simple matter of trying out sticks of different diameters until the message became readable. The art and science of cryptography showed no major changes or advancements until the middle Ages. By that time, all of the western European governments were utilizing cryptography in one form or another. Keeping in touch with ambassadors was the major use of cryptography (Rubin, 2008).

In the 20th century (and arguably until late in that century), cryptography was an art. It focuses solely on the problem of secret communication. Constructing good codes, or breaking existing ones, relied on creativity and personal skill. There was very little theory that could be relied upon and there was not even a well-defined notion of what constitutes a good code (Katz and Lindell, 2007). Academic research in cryptology started in the mid-1970s; today it is a mature research discipline with an established professional organization (IACR, International Association for Cryptologic Research), thousands of researchers, and dozens of international conferences. Every year more than a thousand scientific papers are published on cryptology and its applications. As cryptology is moving fast, it is hard to keep up with all the developments (Paar, and Pelzl, 2010).

In the information age, cryptography has become one of the major methods for protection in all applications. Applications of cryptography include Automated

Teller Machine (ATM) cards, computer password and electronic commerce. In many organizations, Cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). Simpson (1997) remarked that, "cryptography is a primary method of protecting valuable electronic information in many organizations". For a website in an organization to be secured all of the data transmitted between the computers where the data is kept and where it is received must be encrypted.

Security mechanisms that rely on cryptography are an integral part of almost any computer system in most organizations. Users (often unknowingly) rely on cryptography every time they access a secured website. Cryptographic methods are used to enforce access control in multi-user operating systems, and to prevent thieves from extracting sensitive information from stolen laptops. Software protection methods employ encryption and other tools to prevent unauthorized copying of valuable records (Katz and Lindell, 2007). The basic functions of cryptography are encryption and decryption..

Encryption

Encrypt means to convert (information or data) into a code, especially to prevent unauthorized access. Encryption can be defined as the conversion of plain message into a form called a ciphertext that cannot be read by anyone without decrypting the encrypted text (Justin and Manimurugan, 2012). Encryption is the coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key. Encryption is used in an institution

secure Websites as well as other mediums of data transfer. If intruders were to intercept the information you sent via an encrypted connection, they would not be able to read it (Techterm, 2013).

According to Mahmud (2004) the two basic building blocks of all encryption techniques are Substitution and Transposition. A Substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. Transposition technique is a different kind of mapping where mapping is achieved by performing some sort of permutation on the plaintext letter i.e. In transposition techniques plain letters are simply rearranged**.**

Decryption

Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plaintext, so that it can be read (Justin and Manimurugan, 2012). According to Bolton (2013), decryption means extracting the original information from the encrypted data. The complexity of the algorithm used means that a strongly encrypted message might require thousands of years of processing by very fast computers to break the encryption.

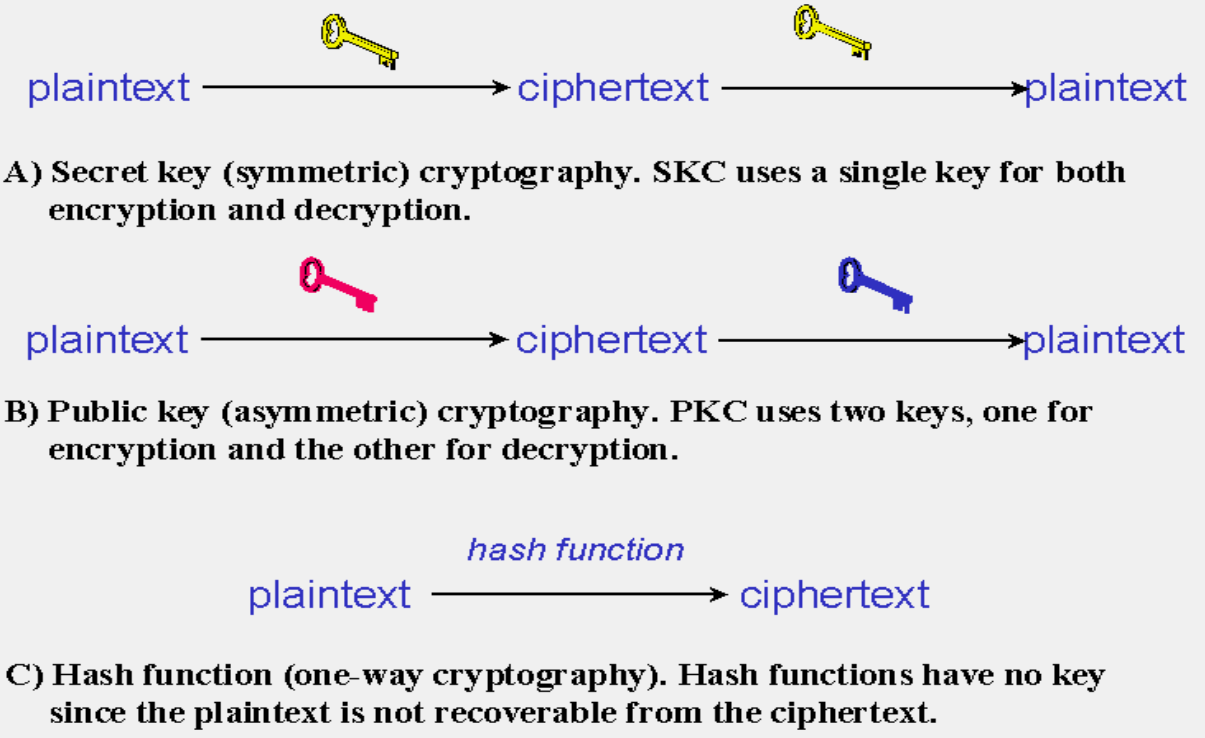
Cryptosystems in Modern Cryptography

A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption i.e. a cryptographic algorithm, plaintexts, ciphertexts, and keys (Jarvinen, 2008).

Types of Cryptographic Techniques

According to Kessler (2013) the three common types of cryptography are: Symmetric Key Cryptography, Public-key Cryptography, and Hash Function Cryptography as shown below:

Figure 2.2 Types of Cryptography: Secret-Key, Public Key, and Hash Function

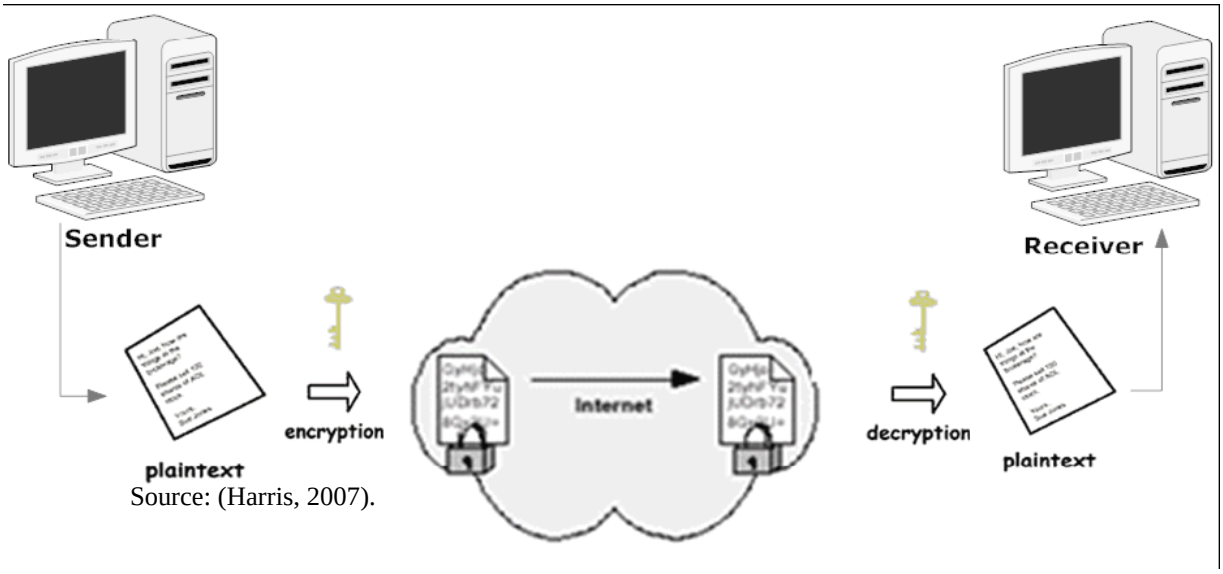


Source: (Kessler, 2013).

❖ **Symmetric (Secret-Key) Cryptography**

With secret key cryptography, a single key is used for both encryption and decryption. As shown in figure 2.2. A. above, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key (Kessler, 2013).

Figure 2.3 Symmetric (Secret-Key) Cryptography



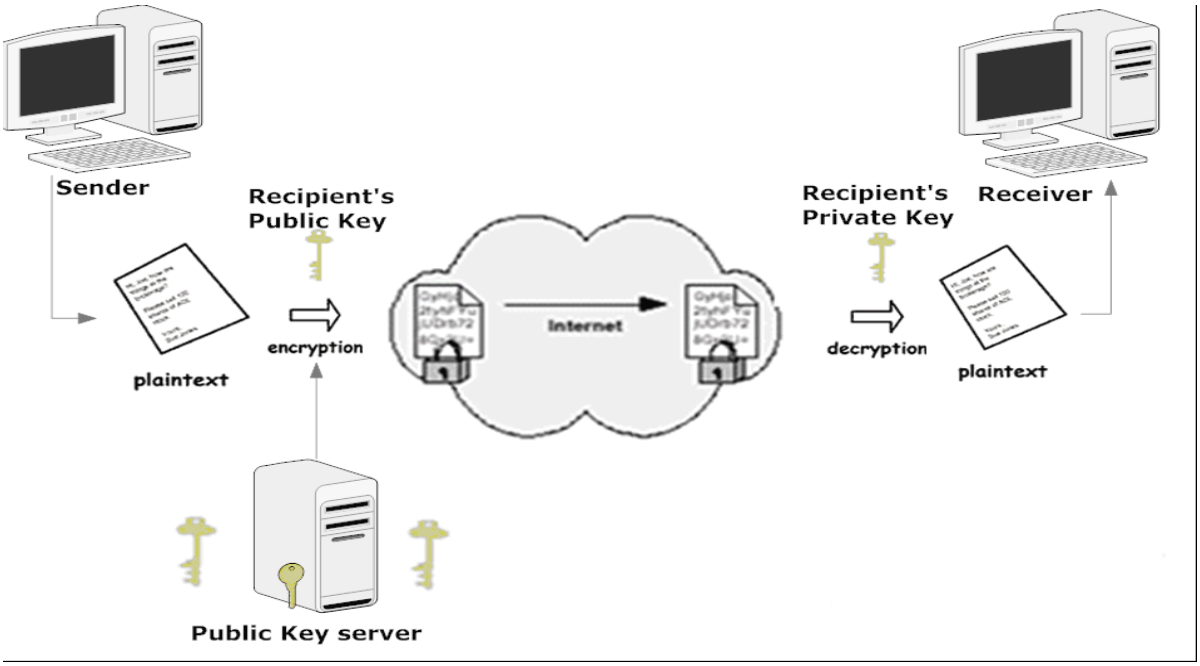
Source: (Harris, 2007).

❖ **Asymmetric (Public-Key) Cryptography**

Public-key cryptography (PKC) has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work (Figure 2.2 B). Because pair of keys is required, this approach is also called asymmetric cryptography. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his

private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message and Alice cannot deny having sent the message i.e. non-repudiation (Kessler, 2013).

Figure 2.4 Asymmetric (Public-Key) Cryptography



Source: (Harris, 2007)

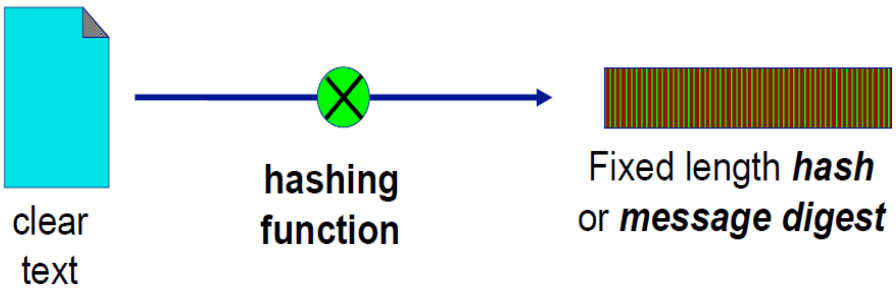
❖ **Hash Functions (One-Way Cryptography)**

Hash functions, also called message digests and one-way encryption, and are algorithms that, in some sense, use no key (Figure 2.2 C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating

systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file (Kessler, 2013).

A common role played by hashing in modern cryptosystems is improving the efficiency of digital signatures. Because public-key ciphers are much slower than symmetric ciphers, signing large blocks of data is very time-consuming. Instead, most digital signature protocols specify that the digital signature is instead applied to a hash of the data. Given that computing a hash is generally fast and the resulting value is typically much smaller than the data, the signing time is drastically reduced. Other common uses of cryptographic hashes include protecting passwords, time-stamping data to securely track creation and modification dates and times, and assuring data integrity. The well-known Secure Hash Algorithm family includes SHA-224, SHA-256, SHA-384, and SHA-512. The older SHA-1 and MD5 algorithms are currently in wider use, but flaws in both have been identified, and both should be retired in favor of a more secure hash. Hash functions provide a measure of the integrity of a file (Kevin, 2006).

Figure 2.5 Hashing (One-Way Cryptography)



Source: (Schneier, 1996).

2.3 Types of Databases Available and Accessible

The introduction of computers together with the development of the Internet technology has change how organizations handle and secure their information. Today many organizations adopted database systems as the key data management technology for decision-making and day-to-day operations. As the data is to be shared among several users the system must avoid anomalous results and ensure the safety of the information stored despite system crashes and attempts at unauthorized access. The data involved here can be highly sensitive or confidential, thus making the security of the data managed by these systems even more crucial as any security breach does not affect only a single application or user but can have disastrous consequences on the entire organization (United Kingdom Essays, 2013).

Before the advent of computer, a file cabinet could be considered a very basic form of a non-digital database. The cabinet contains files (records) that contain filing cards (pieces of information). These pieces of information are placed in some sort of order for easy access. Within an electronic database, a computer program assists the user in locating requested pieces of data.

According to Pennsylvania State University (2012) an electronic database is much like a non-electronic database, except that data is stored on a computer or computer server. The software or database program which houses the data typically allows a number of operations which make searching records much easier. These include:

a. Quick, targeted filter/finds/search - allows users to search exactly on the criteria they are interested in.

b. Multiple sorts - applications allow often allow users to see the same data or data subset in different sort orders.
c. Validation (error proofing) - it is possible to program data entry forms so that users enter data consistently instead of using different codes on the fly.
d. Export/import - databases can import large chunks of data from another data source in one operation.
e. Automatic calculations - databases, especially those with a focus on statistics or finances, can be programmed to perform complex calculations automatically.
f. Charting - some databases can efficiently plot data points or numerical data in more user friendly charts and graphs.
g. Formatting - some database applications, such as EndNote, can show the same data in a different set of formatting or reporting styles, thus saving users from having to re-type data

Pennsylvania State University (2012) also asserted that Card catalogs were one of the primary examples of a non-electronic database with multiple sorts. Before the advent of the electronic card catalog (the CAT), users wanting to use more than sort had to walk to different sets of card catalogs. If you wanted to search on more than one synonym, you would have to walk to a different alphabetic section of the card catalog. In the electronic version, if you need to search on a different sort, you enter the data into different corresponding fields such as "Author" or "Topic". You can even search on multiple fields such as "Author" and "Date" or even by "Call Number" if you need to see a record for a specific item. If you need to search synonyms, you can just do multiple searches. A half-hour search at multiple card

catalog stations has been replaced by a five-minute session with workstation (or you can search at your computer before even going into the library).

From another perspective, Rodriguez (2014) posited that a database is an electronic file that stores information in a series of records. Records are often contained in one or more tables. There are many types of databases that vary by functions and data models. One way to classify different types of databases is by their functions:

1 Look, but don't touch: Sometimes called On-line Analytical Processes (OLAP) is designed to assist in decision-making. Typically, an OLAP database contains statistical information that is read by users, but not modified.

2 Change is good: also known as On-line Transaction Processing (OLTP) can be manipulated by users. Records can be added, deleted or modified by users with the proper level of access.

Rodriguez (2014) further added that the second way to classify different types of databases is by their "data models." i.e. a data model describes the structure of data and how it is accessed. There are several common data models:

1 Flat-file. Flat file databases most closely resemble paper files and file cabinets. Flat file databases, while simple to create and access, contain lots of redundant information. These redundancies slow down the search process, making the flat-file type of database inefficient.

2 Hierarchical. Hierarchical databases relate tables in a parent/child format. Although this reduces redundancy and increases organization, it is still a

limiting way to handle data. The fact that child tables at the same level do not have links to each other makes searching problematic.

3 Relational. Relational databases link tables with common "key" fields allowing for sophisticated relationships between tables. Table links can be "indexed" or stored for future use, resulting in quicker searches in this type of database.

4 Object-oriented. Object oriented databases are structurally similar to relational databases. While most other types of databases are designed to hold text and numbers, object-oriented databases are designed to store audio, video and other mixed media objects. These types of data are to be secured or must be kept away from hackers.

There are many, many different types of electronic databases in the world today, including full-text databases, bibliographic databases, statistical databases, image databases, and others. Using electronic databases is a very valuable way to conduct research. Before the advent of electronic databases, research was even more time-consuming and tedious. Today, with the proper use of an electronic database, full-text articles appear almost instantaneously on your computer screen. With the advent of the Internet, you may not even need to leave your home to conduct research.

In most tertiary institution, request to access electronic database must be referred to the office responsible for maintaining those data. The institution retains ownership of all management of information created or modified by its employees as part of their job functions. Some tertiary institution' database applications were build using hierarchical and network systems while others

have so many different database systems like relational databases (RDBMS), object-oriented databases (OODBMS), object-relational databases (ORDBMS), eXtended Query (XQUERY); one factor which was, is, and will be of the utmost importance is the security of the data involve.

Data can hamper the functionality of an entire organization in a proper way if not available when needed. Thus the security in terms of databases can be broadly classified into access security and internal security. Access security refers to the mechanisms implemented to restrict any sort of unauthorized access to the database; examples can be authorization methods such as every user has a unique username and password to establish him as a legitimate user when trying to connect to the database. When the user tries to connect to the database the login credentials will be checked against a set of usernames and password combinations setup under a security rule by a security administrator. Internal security can be referred to as an extra level of security, which comes into picture if someone has already breached the access security such as getting hold of a valid username and password, which can help getting access to the database. So the security mechanism implemented within the database such as encrypting the data inside the database can be classed as internal security, which prevents the data to be compromised even if someone has got unauthorized access to the database (United Kingdom Essays, 2013).

2.4 Security Threats faced by Databases

In a world where data is everywhere, the need to protect the vital information is very essential. Complex, heterogeneous IT environments make data breach and threat response very difficult. The threat represents the type of action

that is likely to be of harm (Kioskea, 2013). A threat is something which potentially violates security. It exists when there is a circumstance, capability, action or event that could breach security and cause harm i.e. is a possible danger that might exploit vulnerability,

Schneider (2013) explains threat as: Any potential danger to information or systems that someone would identify and exploit the vulnerability. The entity that takes advantage of vulnerability is referred to as a threat agent. Miessler (2013) posited that a threat is an event, natural or man-made, that can cause damage to your system. Threats include people trying to break into your network to steal information, fires, tornados, floods, social engineering, malicious employees, etc. Anything that can cause damage to your systems is basically a threat to those systems.

Kayarkar (2012) posited that any intentional or accidental event that can adversely affect a database system is considered as a threat to database and database security can be defined as a mechanism that protects the database against such intentional or accidental threats. Some security threats affect database includes:

i. **Privilege Abuse:** When database users are provided excessive privileges than their required functionality, then these privileges can be intentionally or unintentionally exploited.

ii. **Legitimate Privilege Abuse:** In this attack, the attacker with the legitimate privilege access to the database may abuse the information stored in the database for the malicious purposes.

iii. **Privilege Promotion:** The attacker in this attack takes advantage of the software vulnerabilities and errors and then elevates his clearance level to access the critical information stored in the database.

iv. **Operating System Vulnerabilities:** In operating system vulnerabilities, the attacker exploits the vulnerabilities in the operating system to gain unauthorized access to the database for malicious reasons.

Similarly, Schneier (1997) postulated that the security threats to electronic databases include the following:

1. Data Tampering
2. Eavesdropping and Data Theft
3. Falsifying User Identities
4. Password-Related Threats
5. Unauthorized Access to Tables and Columns
6. Unauthorized Access to Data Rows
7. Lack of Accountability
8. Complex User Management Requirements.

Every organization needs to identify the threats they might be subjected to and the subsequently appropriate security plans and countermeasures should be taken, taking into consideration their implementation costs and effects on performance. Addressing these threats helps the enterprise to meet the compliance and risk mitigation requirements of the most regulated industries in the world.

To know the potential threats at an entry point in tertiary insitution, for that one must identify any security-critical activities that can occur and imagine what an adversary might do to attack or misuse insitution database system. This can be

realized by asking questions such as How could the adversary use a technicques to modify and control the database system, retrieve restricted information, manipulate information within the database system, cause the system to fail or be unusable, or gain additional rights in the institution. In this way, one can identify the chances of the adversary accessing the information in the insitution database system without being audited, skipping any access control checks, or appearing to be another user (Anley, 2002).

2.5 Cryptography Prevention of Security Breach

Security is the quality or state of being secured, to be free from danger. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective . According to Steve (2007) security breaches can be classified as unauthorized data observation, incorrect data modification, and data unavailability, which can lead to loss of confidentiality, availability, integrity, privacy, theft and fraud. Unauthorized data observation results in disclosure of information to users who might not be entitled to have access to such kind of information. Cryptography is used to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.

According to Symantec (2009) there are three main types of security breaches: well-meaning insiders, targeted attacks, and malicious insiders. In many cases, breaches are caused by a combination of these factors:

- **Well-meaning insiders**

A staff in an organization who inadvertently violate data security policies continue to represent the largest population of data breaches. An analysis of

breaches that can be caused by well-meaning insiders in company or organization yields five main types:

i. **Data exposed on servers and desktops:** Semantec (2009) further explain that daily proliferation of sensitive information on unprotected servers, desktops, and laptops is the natural result of a highly productive workforce. Perhaps the most common type of data breach occurs when well-meaning insiders, unaware of organization data security policies, store, send, or copy sensitive information unencrypted in the database. In the event a hacker gains access to your network, confidential files stored or used without encryption are vulnerable and can be captured by hackers. As a result of data proliferation, most organizations today have no way of knowing how much sensitive data exists on their systems.

ii. **Lost or stolen laptops:** Lost laptops in organizations were the top cause of data breaches. Even when such cases do not result in identity theft, data breach disclosure laws make lost laptops a source of public embarrassment and considerable expense.

iii. **Email and removable devices.** Unencrypted network transmissions create significant risk of data loss. In a typical scenario, an employee sends confidential data to a home email account or copies it to a memory stick or CD/DVD for weekend work. In this scenario, the data is exposed to attack both during transmission and on the potentially unprotected home system or removable media device.

iv. **Data loss incidents:** When data sharing is overly extensive or when users fail to enforce data security policies, the risk of data breaches increase.

v. **Processing of organization records automate the spread of sensitive data:** One reason for proliferation of confidential data is inappropriate processing automatically distribute such data to unauthorized individuals or unprotected systems, where it can be easily captured by hackers or stolen by malicious insiders.

❖ **Targeted Attacks**

In today's connected world where data is everywhere and the perimeter can be anywhere protecting information assets from sophisticated hacking techniques is an extremely tough challenge in most organizations. Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. Some attacks are often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites through one of four ways:

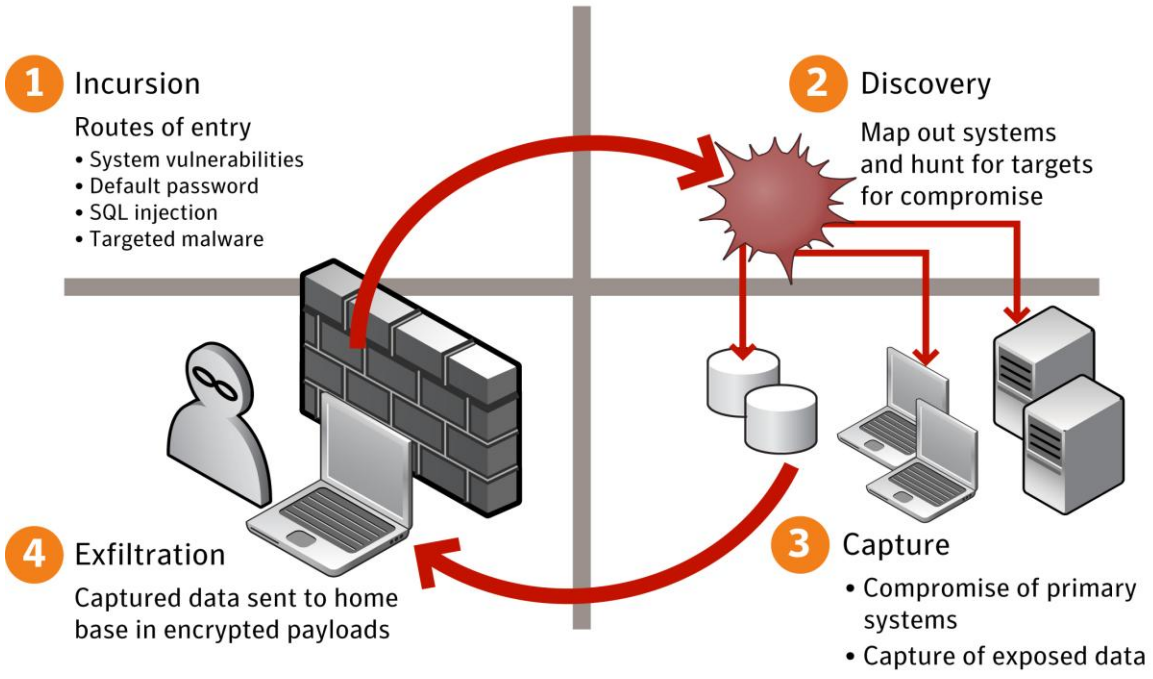
i. **System vulnerabilities:** Many times organizations laptops, desktops and servers do not have the latest security patches deployed which creates a gap in an overall security posture. Gaps or system vulnerabilities can also be created by improper computer or security configurations. Cybercriminals search for and exploit these weaknesses in order to gain access to the corporate network and confidential information.

ii. **Improper credentials:** In many organizations, passwords on Internet-facing systems such as email, web servers are often left on factory default settings, which are easily obtained by hackers.

iii. **SQL injection:** by analyzing the Universal Remote Locator (URL) syntax of targeted websites in organization, hackers are able to embed instructions to upload spyware that gives them remote access to the target servers.

iv. **Targeted malware:** Hackers use spam, email and instant message communications often disguised as known entities to direct users to websites that are compromised with malware. Once a user visits a compromised website, malware can be downloaded with or without the user's knowledge. Gimmicks such as free software deceive users into downloading spyware that can be used to monitor user activity on the web and capture frequently used credentials such as users' logins and passwords. Remote access tools (RATs) are an example of spyware that is automatically downloaded to a user's machine without their knowledge, silently providing the hacker control of the user's computer and access to organization' information from a remote location.

Figure 2.6 Phases of Targeted Attack



❖ **The Malicious Insider**

Malicious insiders constitute drivers for a growing segment of data breaches. Breaches caused by insiders with intent to steal organizations' information fall into four groups:

i. **Sabotage staff crime:** The staff who knowingly steals data as part of an identity theft ring has become a highly notarized figure in the current annals of crime in most organizations. Such operations are perpetrated by insiders who abuse their privileged access to information for the purpose of personal gain.

ii. **Terminated employees:** Data breaches caused by disgruntled former employees have become commonplace in organizations. Often, the employee is notified of his or her termination before entitlements such as Active Directory and Exchange access have been turned off of the organizations, leaving a window of opportunity in which the employee can access confidential data and email it to a private account or copy it to removable media.

iii. **Career building with organizations data:** It is common for a staff to store organization data on a home system in order to build a library of work samples for future career opportunities. While the motives for such actions may not be considered malicious on the order of identity theft, the effect can be just as harmful. If the employee's home system is hacked and the data stolen, the same damage to the organization can ensue.

iv. **Organization espionage:** The final type of malicious insider is the unhappy or underperforming employee who plans to send out secrect organization's information to the criminal to gain money.

Most organization are negligent in security practices, allowing hackers to gain control of portions of their networks through fairly simple means.The most expensive computer crime is denial of service and theft of intellectual property and the most common security breaches in most organizations are caused by automated attacks, such as Worms, Viruses, and Trojans (Kabay, 2004).

Prevent, detect, and mitigate breach is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS (distributed denial-of-service) detection and prevention, and multi-factor authentication for service access. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and segregation of the employee email environment from the production access environment (Kessler, 2013).

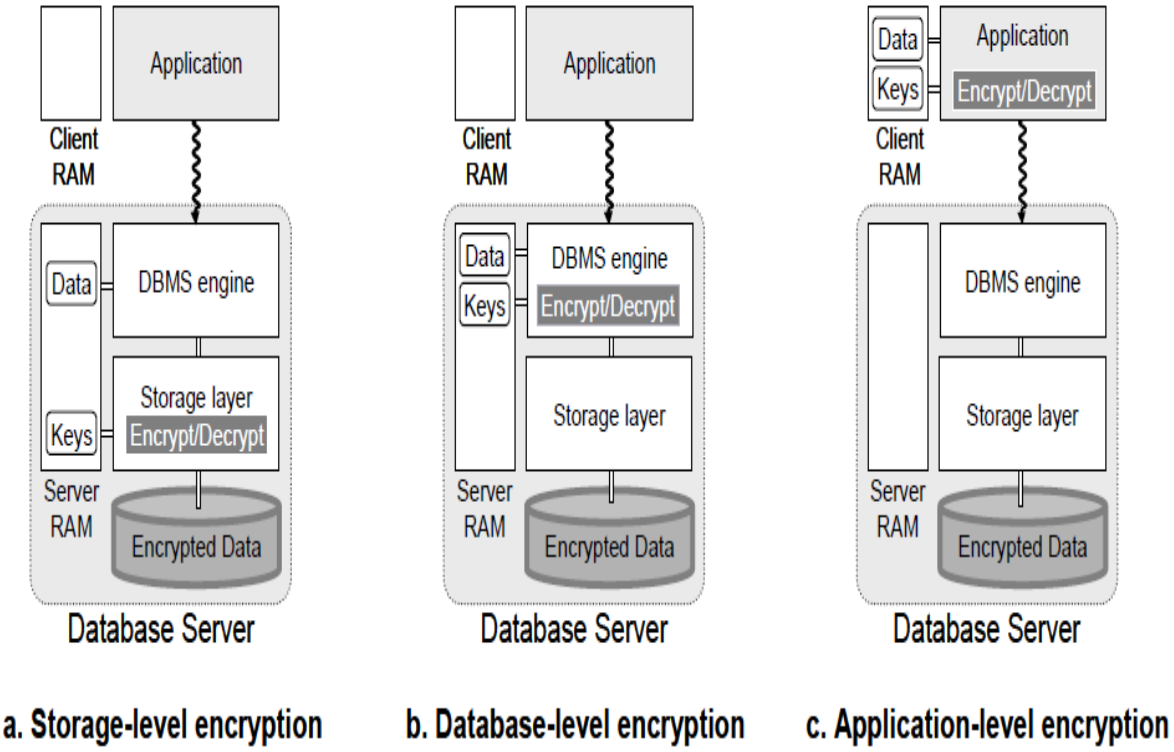
The unprecedented surge in data security breaches is forcing organizations to face a discouraging reality: A breach prevention strategy is not protecting the data. In fact, increased investment in perimeter-based security only exacerbates the problem because it fails to address the core of the issue. Namely, that the nature of data has changed. No longer just contained within an on-premise data center, data is constantly being accessed, moved, shared and stored in virtualized academic environments which create vast new points of vulnerability (SafeNet, 2014).

As data breaches continue to plague organizations and the impacts to individuals increase, the statutory and regulatory responses become more severe. Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it. Cryptography is one of the techniques of encoding data, so that only authorized users can understand it. Encryption alone, however, is not sufficient to secure your data. Protecting data in the database includes access control, data integrity, encryption, and auditing. Encryption is so important for data security. Even if an intruder could gain access to institutions' network or even mobile device containing sensitive data, the data would be unreadable unless they also had access to the encryption key that unscrambles the data (Schneier, 1997). A reality that renders organizations IT security strategies founded on breach prevention. By encrypting the data itself and focusing on the highest risk-profile environments there is need to provide a data security strategy that makes breaches irrelevant, simply because encrypted data loss is really no loss at all. Data encryption solutions are built on a proven and scalable crypto foundation that makes it possible to efficiently protect the data assets themselves allowing organizations' data to move freely and securely through any medium (SafeNet, 2014).

According to Kayarkar (2012) modern cryptography prevents sensitive data from wrong hands in almost all kinds of attacks. Database encryption is the process of converting data, within a database, in plain text format into a meaningless cipher text by means of a suitable algorithm. The database encryption protects the stored data. It provides strong security for data, but developing a database encryption strategy must take many factors into consideration:

- **Storage-level encryption:** amounts to encrypt data in the storage subsystem and thus protects the data at rest (e.g., from storage media theft).
- **Database-level encryption:** allows securing the data as it is inserted to, or retrieved from the database.
- **Application-level encryption:** moves the encryption or decryption process to the applications that generate the data. As shown in figure 2.7 below:

Figure 2.7: Strategies For Database Encryption



Source: (Kayarkar, 2012).

An organization can choose to encrypt data at the application level, the database level, or the storage level. Encryption at the lowest of these levels, the storage level on the disk or tape guards against risk in the case where storage media are lost, but it does little to protect against malicious insiders or systems infected by

malware. Application-level encryption on the other hand represents the other extreme by providing the highest degree of control, but it may not always be a viable approach. Because of these tradeoffs, many organizations are increasingly turning to database encryption as offering the best of both worlds when it comes to protecting data at rest, the protection goes further than storage level encryption and also avoids widespread changes in the application layer.

2.6 Challenges Encountered in the Application of Cryptography

When security safeguards are not adequate, trespassers run little risk of getting caught. They can attack a system using techniques the designers never even considered. They steal data, bribe insiders, modify software, and collude. The odds favor these attackers. Bad guys have more to gain by thoroughly examining a system than the good guys do. Defenders must protect their system against any possible vulnerability, but an attacker need only find one security flaw to compromise the whole system. While no one can guarantee 100% security, cryptography can help significantly. The good news is that if an organization already has the algorithms and protocols it can secure its systems; the bad news is that implementing the protocols successfully requires considerable expertise (Schneier, 1997).

The popularization of the Internet has brought fundamental changes to the world, because it allows a universal method of communication between computers. This carries enormous benefits with it, but also raises many security considerations. Cryptography is a fundamental technology used to provide security of computer networks, and there is currently a widespread engineering effort to incorporate cryptography into various aspects of the Internet. Most of the difficulty in

engineering cryptographic systems has to do with understanding the trust relationships between different entities involved in a protocol (Murphy and Badger, 1996).

Data security and the challenges of data protection are increasing in scope and difficulty. While many organizations have long needed to safeguard intellectual property and confidential information, changes in information technology and business models introduce new actors, new threats, and new regulations. As a result organizations need to think beyond the traditional models of securing the perimeter and locking down specific segments of IT infrastructure in order to formulate their data protection goals. Some inherent challenges to application of cryptography include the following:

1. Strength of encryption (algorithm, key size)
2. Quality of encryption (sufficiently reviewed by experts)
3. Implementations subjected to accreditation
4. Speed of encryption
5. Management of the persistent encryption keys
6. Randomness (use of random number generator) jargon

The aforementioned must be implemented perfectly, or the system will fail. A poorly designed user interface can make a hard-drive encryption program completely insecure. Under deadline and budget pressures, implementers use bad random- number generators, do not check properly for error conditions, and leave secret information in swap files. Since such mistakes are not apparent in testing, they end up in finished products. More often than not, organizations fail to catch these subtleties and implement insecure algorithms and protocols. The areas of

security with which people interact with key management, human/computer interface security, access control often defy analysis. And the disciplines of public-key infrastructure software security, computer security, network security, and tamper-resistant hardware design are very poorly understood. Design work is the mainstay of the science of cryptography, and it's very specialized. Cryptography blends several areas of mathematics: number theory, complexity theory, information theory, probability theory, abstract algebra, and formal analysis. Few can do the science properly, and a little knowledge is a dangerous thing: Inexperienced cryptographers almost always design flawed systems. Nothing substitutes for extensive peer review and years of analysis (Schneier, 1997).

McCurley (1996) opined that the challenges to application of cryptography include:

1. Encryption is not a silver bullet for protecting data; it can be applied in a wide variety of ways to protect a wide variety of data types. Most likely it will be applied in layers, with each layer playing an important role. Failure to adopt a strategic approach will result in increased costs, complexity, and business risk.
2. It can be easy to focus on encryption and overlook the issue of key management. Encryption technology itself is mature, some would say commoditized.
3. Compliance requirements and auditors are increasingly tuned to the issues of key management; to avoid falling behind, organizations should be ready to demonstrate their adherence to best practices or other standards of due care.
4. The risk of key theft may be smaller than the risk of losing keys and therefore losing the data they protect. Human error is common, particularly in situations

where key management relies on manual processes, poor documentation, and poorly trained staff.

5. Encryption can often be a computationally intensive process that can degrade performance of servers, gateways, and other application platforms. If not implemented in an optimal way, encryption can limit capacity, drive up costs, and adversely impact the user experience.
6. Scalable cryptographic primitives: For many applications, our current state of knowledge concerning the amount of computation required to carry out various cryptographic primitives will severely limit the application of cryptography in the future. While computers continue to get faster at an astounding rate, there is still a continuing need to explore the boundaries on what the minimal amount of computation and communication required to perform specific cryptographic tasks. Examples include cryptographic hashing, key exchange, digital signature construction and verification, batch processing, and basic encryption.
7. Electronic Commerce Issues: The primary reason for a rising interest by society in the Internet is directly derived from the perception that the Internet offers a promise of new ways to conduct commerce. An ubiquitous communication infrastructure provides a convenient way to offer information products and contact customers for electronic commerce.
8. Denial of Service Attacks: The ability to freely communicate with a vast number of parties leads to the need for parties to protect themselves against denial of service attacks.

2.7 Summary of the Review

The chapter identified, reviewed, analyzed and summarized related and relevant scholarly materials on the general problem of securing information taking into cognizance the security systems (application of cryptography as a reliable means of securing all forms of information) and types of databases available and accessible, the security threat faced by databases as well as the prevention of security breach by cryptography vis-à-vis the challenges encountered in the application of cryptography.

References

Abomhara, M. (2011). Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard. Unpublished MSc. Thesis: University of Malaya.

Adekeye, W.U (1997). *The Importance of Management Information Systems.* University of Ilorin, Ilorin, Nigeria.

Anley C. (2002). Advanced SQL Injection in SQL Server Applications. White paper, Next Generation Security Software Ltd. London.

Bolton, D. (2013). *Definition of Encryption*. Retrieved 3rd May, 2013 from cplus.about.com/od/glossal1/g/algoriyhm.htm.

Buaki, J. (2013). Information System Security Best Practice. Retrieved 5 May, 2013 from http//www.about.com.

Chaudhuri, S., Narasayya, V., (1997). An Efficient, Cost-Driver Index Selection Tool for Microsoft SQL Server," *Proceedings of the 23rd VLDB Conference*, Athens, Greece.

David, K. (2004). Effective Oracle Database 10g Security, McGraw-Hill.

Harris, S. (2007). CISSP® All-in-One Exam Guide. McGraw-Hill.

Jarvinen, K. (2008). Studies on efficient implementation of cryptographic algorithms. Unpublished thesis for the degree of Doctor of Science in Technology, Helsinki University of Technology.

John, W., and Joe, P. (2002). Strategic Planning for Information System. 3rd Ed. West Sussex. John wiley & Sons Ltd.

Justin, M. and Manimurugan, S. (2012). Survey on Various Encryption Techniques, *International Journal of Soft Computing and Engineering* .ISSN: 2231-2307, Volume-2, Issue-1

Kabay, M. (2004). *What's Important for Information Security.* Retrieved 11, May, 2013 from http://www.mekabay.com/overviews/infosec_ed.htm .

Katz, J. and Lindell, Y (2007). Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall/CRC , Boca Raton London New York.

Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. M.G.M's College of Engineering and Technology, Navi Mumbai, India

Kenan, K. (2005). Cryptography in the Database: The Last Line of Defense. Retrieved July, 2013, from Http://www.awprofessional/bookstore/product.asp

Kessler, G. (2013). *An Overview of Cryptography*. Retrieved 8th May, 2013 from http://www.garykessler.net/kumquat_pubkey.html.

Kioskea (2013). Introduction to Information Technology Security. Retrieved on May, 2013. From http://www.facebook.com/pages/Kioskea/117422445065179.

Kremlin (2008). Concept of Cryptography. Retrieved 12th April, 2014.From http://www.kremlinencrypt.com/concepts.htm

Mahmud, S. (2004). A study on Parallel Implementation of Advanced Encryption Standard (AES). Unpublished M.Sc Thesis in Independent University, Bangladesh.

McCurley, K. S. (1996). Cryptography and the Internet: Lessons and Challenges. Retrieved 24th March, 2014 from http://www.mccurley.org/papers/asiacrypt96/

Menezes, A.J. Van Oorschot, P.C. And Vanstone, S.A. (1997). *Handbook of Applied Cryptography*. London: CRC Press.

Miessler, D. (2013). An Information Security Concepts Primer. Retrieved on 9th May, 2013. From http//creativecommon.org.

Murphy. S and Badger, M. (1996). ``Digital Signature Protection of the OSPF Routing Protocol", Proceedings of the 1996 Symposium on Network and Distributed Systems Security, IEEE,

Paar. C and Pelzl. J. (2010). Understanding Cryptography. Springer Heidelberg Dordrecht London.

Pawlan, M. (1998). Cryptography: the ancient art of secret messages. Retrieved May 4, 2013, from http://www.pawlan.com/Monica/crypto/

Pell, O. (2013). A brief History of Cryptography and Cryptology. Retrieved 0n 8th May, 2013 from http:// www. Doc.ic.uk.

Ramakrishnan, P. (2003). Information Security Management Systems. Retrieved on 13 May, 2013frommhtml:file://E:\Whitepaper\Information%20Security%20Management%20Systems.mh.

Richardson, R. (2008). CSI Computer Crime and Security Survey. California: Irvine.

Rodriguez, G. (2014). What are the Most Common Types of Databases. Retrieved on 14TH January, 2014 from http://www.life123.com/author/gene_rodriguez,_iii

Ronald, L. (1990). *Handbook of Theoretical Computer Science* 1. Elsevier.

Rouse, M. (2007). *Security Policy*. Retrieved 9th May, 2013 from http://whatis.techtarget.com/contributor/Margaret-Rouse

Ruskwig (2011). Security Policies. Retrieved 10th May, 2013, from http://www.ruskwig.com/it security policy.htm.

Rubin, J. (2008). Vigenere Cipher. Retrieved May 4, 2013, from http://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html.

SafeNet (2014). Data Encryption Solutions. Retrieved 24th March, 2014, from http://www.securethebreach.com/

Savu, L. (2013). Cryptography Role in Information Security. University of Bucharest Bucharest, Romania.

Schneider, L. (2013). Information Security - Learn about Information Security. Retrieved on 18th April, 2013 from *http://www.about.com/*.

Schneier, B. (1996). Applied Cryptography. New York: Wiley.

Schneier, B. (1997). Cryptography, Security and the Future. Retrieved 10th April, 2014. From http://www/schnnier.com/cryptography.html.

Simpson, S. (1997). Cryptography in Everyday Life. Retrieved 6th May, 2013 from www.laist.com.edu.

Stallings, W. (2003). Cryptography and Network Security: Principles and Practices. Third Edition, Pearson Education, Inc.

Steve, G. (2007). Databases for Embedded Systems. *Embedded Computing Design* magazine. Retrieved on August 13, 2013 from http//www.embedded-computing.com

Sudarshan, K.S. (2001). Database System Concepts, Fourth Edition, McGraw−Hill Companies.

Symantec (2009). Anatomy of a Data Breach: Why Breaches Happen and What to Do about It. Symantec World Headquarters 350 Ellis St. Mountain View, USA.

Taylor, K. (2002). Number Theory 1. Retrieved May 4, 2013, from http://math.usask.ca/encryption/lessons/lesson00/page1.html.

Techterm.com (2013). *Definition of cryptography*. Retrieved May 3rd, 2013, from www.techterms.com/category/technical.

Techopedia (2011). *The Seven Basic Principle of IT Security* Retrieved 7th, May, 2013 from http// www.techopedia.com.

TechTarget (2011). Encryption techniques and products for hardware-based data storage security. Retrieved 8 may, 2013 from http://www.computerweekly.com/about/copyright.

United Kingdom Essays (2013). Database Security and Encryption. Retrieved 5th July, http://www.ukessays.com/

Wayne, M. (1998). *Cryptography and Liberty*. Retrieved from http://www.gilc.org/ on 3rd May, Security+ Certification: Exam Guide. McGraw-Hill.

Whitman, M. and Mattord, H. (2005). *Principles of Information Security*. University of Phoenix Custom Edition e-text. Canada, Thomson Learning, Inc. Retrieved May 4th, 2013, from University of Phoenix, rEsource, CMGT/432.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the research methodology employed in conducting the study, population of the study, sample and sampling techniques, instruments for data collection, validity of the instruments, reliability of the instruments, method for data collection as well as the procedure for data analysis.

The chapter is presented under the following sub headings:

3.2 Research Method Adopted for the Study

3.3 Population of the Study

3.4 Sample and Sampling Techniques

3.5 Instruments for Data Collection

3.6 Validity of the Instruments

3.7 Reliability of the Instruments

3.8 Method for Data Collection

3.9 Procedure for Data Analysis

3.2 Research Method Adopted For the Study

Survey research method was adopted in carrying out this study. Benbasat (1980) posited that survey is carried out when an investigator is interested in a single research object and attempts to gather extensive data about it. Isangedi and Ogomaka (1992) observed that the approach allows a concentrated focus on a single phenomenon. Thomas (1996) asserted that, a survey research is a procedure in which information is collected systematically about a set of cases (such as people, organization or objects). Creswell (2003) remarked that, a survey research is a set of

orderly procedures specifying the information to be obtained and from who and how. It provides a quantitative or numeric description of trends, attitudes, or opinion of a description of population. According to Osuala (2005), a survey has the advantage of "studying both large and small population".

In line with the above assertions, a survey research method was to be found to be most appropriate in the application of cryptography for information security in Umaru Musa Yar'adua University, Katsina.

3.3 Population of the Study

The population of this study consisted of the staff of the Directorate of Information and Communication Technology (DICT) in Umaru Musa Yar'adua University, Katsina (UMYUK). According to UMYUK Registry Unit (2014), there are 21 staff in the DICT of the UMYUK. Therefore, the entire 21 staff members of the DICT were the target population for this study. The choice of the DICT staff in this study was informed by the fact that, they were the people involved in managing the electronic databases of the University**.** In addition, they form the major group who are likely to provide the information required for the study. Omotosho (1991) remarked that population is the "total number of objects in an area of interest and that they must be constable and may be finite or infinite". Osuala (2005) also argued that "population is a means of identifying characteristics which members of the universe have in common and which will identify each unit as identifying a member of a particular group".

3.4 Sample and Sampling Techniques

The fact that the population of this study is not large the entire 21 staff of DICT in Umaru Musa Yar'adua University, Katsina were used in carrying out this study. This is in line with Benard (2012) who asserted that "if a population of a study is less than two hundred (200) the entire population should be used for the study". Hence, no sampling technique was applied.

3.5 Instruments for Data Collection

In carrying out this study, two instruments, namely; questionnaire and observation techniques were used for collecting data. Mohammed (2003) posited that, questionnaire and observations are used due to convenience and their capacity to complement and supplement each other to bridge information gaps likely to be created in finding the relevant information/data for the study.

3.5.1 Questionnaire

Questionnaire has the advantage of gathering information on knowledge, attitude, behaviors, facts and other information (Radhakrishna, 2007).

One type of structured questionnaire was constructed for DICT Staff of the UMYUK. The questionnaire was divided into seven sections: Section A contained personal data of the respondents; Section B Types of database systems available and accessible, Section C Security threats to databases; Section D Extent of cryptography prevention of security breach in databases and Section E Challenges encountered in the application of cryptography.

3.5.2 Observation Technique

The researcher used the observation technique as another tool to gather information on the Application of Cryptography for Information Security in UMYUK. Ekeh (2003) reported that "to observe means to watch carefully for the occurrence of variables, measure and record for the purpose of relating it to other variables". The choice of this instrument was based on the fact that observational method can exert varying amount of control over the environment in which the observation takes place. This is in line with Osuala (2005) who asserted that "to rely on the willingness and ability of respondents to report accurately. Data collected by observation, therefore are more objective and usually more accurate".

3.6 Validity of the Instruments

In order to ensure that the instrument is capable of eliciting the required data and information from respondents; it was subjected to face validation by experts to check and make necessary observations, corrections and amendments to strengthen the instrument (Aliyu, 2011). Thus, the questionnaire developed for this study was validated by supervisor(s), professional librarians and research experts to ascertain their construct, face and content validity in order to allow for reliability of use.

3.7 Reliability of the Instruments

Pilot test was conducted in Federal University Dutsin-ma, Katsina State to determine the reliability of the instrument. Ten (10) copies of questionnaire were administered to ICT staff and Split-Half method was observed using odd and even numbers. Spearman Rank Order Correlation formula was used . The result of the test indicated that reliability coefficient of the instrument was found to be 0.78.

Sambo (2008) asserted that in correlation, when the r falls between 0.7, 0.8, and 0.9 or around, there was strong positive correlation. Thus, the instrument was reliable and therefore suitable for the study.

3.8 Method for Data Collection

Questionnaires were administered to the respondents by the researcher and a trained research assistant. Period of two weeks were given to the respondents to adequately respond to the questionnaire items. Also, physical observation was employed in the research by visiting the UMYUK; interacted with the DICT staff; observed the environment and facilities in order to obtain a first-hand information.

3.9 Procedure for Data Analysis

The data collected for this research were presented and analyzed using descriptive statistics and inferential statistics in order to obtain answers to the research questions formulated and also test the hypotheses respectively. In this regard, frequency distribution tables and simple percentages were used to analyze the data**.** The null hypothesis one was tested using Pearson Product Moment Correlation Co-efficient and null hypothesis two was tested using Chi-Square all at 0.05 level of significance.

References

Aliyu, A. (2011). Information Anxiety Among Internet Users in Ahmadu Bello University, Zaria**.** Unpublished MLS Thesis Work. A.B.U University, Nigeria.

Adedokun, O. M and Ejeh, U.L. (2010). Instruction to Research Method in Geography and Social Sciences. Kaduna: Esonaj Ent. Nig. Ltd.

Benbasat, I. (1980). The Case Research Strategy in Studies in Information System. Retrieved on 26th April, 2014. From http:// www.coba.usf.edu/departments.

Benard, J. (2012). Perfecting Your Research Work. London: Unique Press.

Creswell, J. W. (2003). Research Design, Quantitative, Qualitative and Mixed Method Approaches. Thousand Oaks, California: Sage Publications, Inc.

Ekeh, F. I. (2003). Research Methodology and Statistics in Education. Nsukka: Madol Press. pp72-88.

Isangedighi, A. J. and Ogomaka, M.C. (1992). Education Research Methods. Nigeria: Totan Publishers Limited.

Jen, S. U. (2002). Fundamentals of Research Methodology. Yola: Paraclete Publishers. pp75-81

Mohammed, Z. (2003). A Study of the Status of ICT Availability and Applications in Nigerian Libraries and Information Centres. A Paper Presentation at Ahmadu Bello University Zaria.

Omotosho, A. (1991). Statistics Methods. Ibadan: N.P.S. Educational Publishers Ltd.

Osuala, E. C. (2005). Introduction to Research Methodology. Nimo: Rex Charles and Patrick. pp253-267.

Radhakrishna, R.B. (2007). Tips For Developing and Testing Questionnaires/Instruments. Journal of Extension. Vol. 45 no. 1 pp. 1-4.

Sambo, A.A (2008). Research Methods in Education. Lagos: Sterling Hoden Publishers (Nig) Ltd. Pg 341-354.

Thomas, R. (1996). Survey in Research Methods: Guide For Postgraduate Studies (ed) by Tony Greenfield, London: Arnold.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1 Introduction

This chapter presents the data collected, analysed and discussed according to the research questions and hypothesis raised in the study. The chapter is presented under the following subheadings:

4.2 Response Rate

4.3 Descriptive Statistic Analysis

4.4 Inferential Statistic Analysis

4.2 Response Rate

Out of the twenty one (21) copies of the questionnaire distributed to the Directorate of Information and Communication Technology (DICT) staff in Umaru Musa Yar'adua University, Katsina, twenty (20) were duly completed, retrieved and found useful for analysis. This represents 95.2% response rate. Thus, it is believed that the response rate was good enough to get meaningful data/information necessary for the study. The Table 4.1 below summarises the response rate:

Table 4.1: Response Rate

Directorate	No. of Questionnaire Distributed	No. of Questionnaire Retrieved	% of Questionnaire Retrieved
ICT	21	20	95.2%
Total	**21**	**20**	**95.2%**

Key: ICT = Information and Communication Technology

The high response rate of 20 (95.2%) was realised due to the fact that the researcher administered the instrument personally with the aid of a trained research assistant (ICT staff). It can also be attributed to the fact that the respondents were given up to two weeks to complete and return their copies of questionnaire. Also, a good rapport with the respondents led to the on-the-spot completion of the questionnaire by most of the respondents.

4.3 Descriptive Statistic Analysis

This section analyzed and discussed the data collected with regards to the five research questions raised for this study. Frequencies and percentages were used to compute and present the results. Below is the order of presentation of the collected and analyzed data.

4.3.1 Types of Databases Available and Accessible in Umaru Musa Yar'adua University, Katsina

This research question was raised to identify the types of databases available and accessible in Umaru Musa Yar'adua University Katsina. In order to achieve this objective, a list of electronic databases was outlined for the respondents to tick the databases available in UMYUK. The data collected in this regard were analyzed and presented in Table 4.2 below:

Table 4.2: Types of Databases Available in UMYUK

Types of Databases Available	Yes		NO	
	Freq.	%	Freq.	%
Personnel Records Database	20	100.0	0	0.0
Financial Records Database	20	100.0	0	0.0
Strategic Information Records Database	4	20.0	16	80.0
Students Hostels Records Database	17	85.0	3	15.0
Students Academic Records Database	20	100.0	2	10.0
Medical Records Database	12	60.0	8	40.0

Table 4.2 above has revealed the types of databases available in Umaru Musa Yar'adua University Katsina. It can be seen from the table that personnel records database, financial records database and students academic records database were the types of databases available with the highest frequencies of 100.0% response scores respectively in UMYUK. This is followed by students' hostels records database with the frequencies of 85% response scores.

The implication of this finding is that since students academic records are available and there is no efficient security measure to secure the records, the records can be tempered either by well-meaning insider or targeted attacks. This is in line with the finding of Semantec (2009) who reported that the most common type of data breach occurs when well-meaning insiders, unaware of organization data security policies, store, send, or copy sensitive information unencrypted in the database. In the event a hacker gains access to network, confidential files stored or used without encryption are vulnerable and can be captured by hackers. Also, the

targeted attacks often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites.

However, it was found that 80% of the respondents indicated that strategic information records database was not available in UMYUK. This is surprising because strategic information records database store the important records of the university including, but not limited to, alumni, communication, executive decision making and physical resources.

Also, the researcher sought to determine the types of databases Accessible in Umaru Musa Yar'adua University, Katsina. In order to realize this objective, 5 Points Likert Scale of Measurement was used in this order: Highly Accessible, Accessible, Fairly Accessible, Undecided and Not Accessible. However, for ease of analysis and discussion, the scale was merged into 3 options as shown in Table 4.3 below:

Table 4.3: Types of Databases Accessible in UMYUK

	Accessible		**Undecided**		**Not Accessible**	
Types of Databases Accessible	**Freq.**	**%**	**Freq.**	**%**	**Freq.**	**%**
Personnel Records Database	15	75.0	5	25.0	0	0.0
Financial Records Database	15	75.0	5	25.0	0	0.0
Strategic Information Records Database	3	15.0	1	5.0	16	80.0
Students Hostels Records Database	11	55.0	6	30.0	3	15.0
Students Academic Records Database	16	80.0	4	20.0	0	0.0
Medical Records Database	18	90.0	3	2.0	8	40.0

Table 4.3 above has shown the types of databases accessible by the respondents in Umaru Musa Yar'adua University, Katsina. It was discovered that personnel records database, financial records database, students academic records database and medical records database were the databases that were highly accessible with the highest frequencies of over 70% response scores respectively.

In an academic environment where data are everywhere, the need to protect the confidential information is very essential. Hence, access to these databases should be granted based on the user's need to use specific data and should be subjected to appropriate approval. As such, this access cannot be shared, transferred or deleted. Failure to protect these resources will enable malicious cyber-attacks against sensitive institution's records and increases the potential risk to databases.

On the other hand, 30% of the respondents were undecided on the accessibility of students' hostels records database in UMYUK.

4.3.2 Types of Security Threats that Databases Are Exposed to in Umaru Musa Yar'adua University Katsina

The objective of this research question was to identify the security threats to databases in Umaru Musa Yar'adua University Katsina. To achieve this objective, a list of security threats was outlined for the respondents to tick as many of the threats applicable as shown in Table 4.4 below:

Table 4.4: Types of Security Threats to Databases in UMYUK

Security Threats	Yes		No	
	Freq.	%	Freq.	%
Data Tampering	15	75.0	5	25.0
Password-Related Threats	13	65.0	7	35.0
Worms	13	65.0	7	35.0
Intrusion by Unauthorized Users	14	70.0	6	30.0
Lack of Knowledge of the Security Measures in Place	11	55.0	9	45.0
User Ignorance of the System's Functionalities	12	60.0	8	40.0
Improper Input Validation	9	45.0	11	55.0
Violating the IT Security Policy	8	40.0	12	60.0
Clicking Unnecessary Links	14	70.0	6	30.0
Privilege Abuse	14	70.0	6	30.0
Legitimate Privilege Abuse	8	40.0	12	60.0
Privilege Promotion	10	50.0	10	50.0
Operating System Vulnerabilities	10	50.0	10	50.0

Table 4.4 above has revealed the responses of the respondents on the types of security threats that the databases were exposed to in Umaru Musa Yar'adua University Katsina. Out of the thirteen security threats outlined, only six of them were indicated by the respondents with the highest frequencies of over 60% response scores respectively to have been exposed to the databases in UMYUK. These are data tempering, password-related threats, worms, intrusion by unauthorized users, clicking unnecessary links and privilege abuse.

It was also indicated that, improper input validation, violation of the IT security policy, legitimate privilege abuse were the security threats that were not exposed to databases with the highest frequencies of over 50% response scores respectively in Umaru Musa Yar'adua University Katsina.

Moreover, in order to determine the level of security threats that the database in Umaru Musa Yar'adua University, Katsina were exposed to, a follow up question was raised with respect to this and respondents were asked to indicate the level of security threats using 5 Points Likert Scale of Measurement in the following order: Highly Exposed, Exposed, Fairly Exposed, Undecided and Not Exposed. However, for Researcher's convenience, the options were merged into 3 to ease comprehension in the discussion. Table 4.5 shows the opinion of the responses:

Table 4.5: Level of Security Threats to Database in UMYUK

Security Threats	Exposed		Undecided		Not Exposed	
	Freq.	%	Freq.	%	Freq.	%
Data Tampering	12	60.0	3	15.0	5	25.0
Password-Related Threats	11	55.0	2	10.0	7	35.0
Worms	10	50.0	3	15.0	7	35.0
Intrusion by Unauthorized Users	12	60.0	2	10.0	6	30.0
Lack of Knowledge of the Security Measures in Place	9	45.0	2	10.0	9	45.0
User Ignorance of the System's Functionalities	8	40.0	4	20.0	8	40.0
Improper Input Validation	7	35.0	2	10.0	11	55.0
Violating the IT Security Policy	6	30.0	2	10.0	12	60.0
Clicking Unnecessary Links	11	55.0	3	15	6	30.0
Privilege Abuse	12	60.0	2	10	6	30.0
Legitimate Privilege Abuse	11	55.0	3	15	6	30.0
Privilege Promotion	8	40.0	2	10	10	50.0
Operating System Vulnerabilities	8	40.0	2	10	10	50.0

Table 4.5 above has portrayed the responses of the respondents on the levels of exposure of security threats to the databases in Umaru Musa Yar'adua University Katsina. A careful look at the Table shows that the databases in UMYUK were highly exposed to data tempering, intrusion by unauthorized users, password-related threats, clicking unnecessary links, legitimate privilege abuse and privilege abuse with the highest frequencies of over 50% response scores each respectively. This is followed by worms, user ignorance, and lack of knowledge of the security measures with the frequencies of less than 50% response scores respectively. On the other hand, majority of the respondents indicated that the databases in UMYUK were not exposed to improper input validation, violating the IT security policy, privilege promotion and operating system vulnerabilities with the highest frequencies of over 49% response scores respectively.

However, less than 20% of the respondents were undecided on whether the databases in Umaru Musa Yar'adua University Katsina were highly exposed to security threats or not at all. This finding is surprising considering the fact that the respondents were considered to be highly professionals and skilled in identifying any security threat to their databases and its severity in terms of consequences. This situation might perhaps be attributed also to the simple fact that system security engineer and network engineer were not among the managers of the database systems in Umaru Musa Yar'adua University, Katsina.

4.3.3 Extent of Cryptography Prevention of Security Breach of Databases in Umaru Musa Yar'adua University, Katsina

The objective of this research question was to determine the extent to which cryptography has prevented security breach of databases in UMYUK. In order to achieve this, the researcher first attempted to identify the security breaches experienced in databases in Umaru Musa Yar'adua University, Katsina. To do this, a list of security breaches was provided for the respondents to tick as many security breaches as experienced in databases as shown in table 4.6 below:-

Table 4.6: Types of Security Breaches that Databases Experienced in UMYUK

	Yes		No	
Types of Security Breaches to Databases	**Freq.**	**%**	**Freq.**	**%**
Viruses	13	65.0	7	35.0
Spyware	15	75.0	5	25.0
Denial of Service (DOS) Attack	9	45.0	11	55.0
Distributed Denial of Service (DDOS) Attack	10	50.0	10	50.0
Buffer Overflow Attacks	11	55.0	9	45.0
Brute Force Attacks	8	40.0	12	60.0
SQL Injection	5	25.0	15	75.0
Backup Data Exposure	5	25.0	15	75.0
Database Platform Vulnerabilities	9	45.0	11	55.0
Unauthorized Data Observation	15	75.0	5	25.0
Incorrect Data Modification	18	90.0	2	10.0
Phishing Scams	15	75.0	5	25.0
Social Engineering	10	50.0	10	50.0
Super-Users with Broad Access Rights	9	45.0	11	55.0

Table 4.6 above has shown the responses of the respondents on the types of security breaches experienced by UMYUK on their databases. It was discovered that viruses, spyware, unauthorized data observation, incorrect data modification and phishing scams were the security breaches experienced with the highest frequencies of over 60% response scores respectively. This is followed by, buffer overflow attack with the frequencies of over 50% response scores. This finding is in line with the finding of Steve (2007) who posited that the security breaches can be classified as incorrect data modification, unauthorized data observation, and data unavailability, which can lead to loss of confidentiality, availability, integrity, privacy, theft and fraud. Unauthorized data observation results in disclosure of information to users who might not be entitled to access to such kind of information.

The implication of this finding is that as data breaches continue to plague organizations and the impacts to individuals increase, the statutory and regulatory responses become more severe. This paved way for cybercrimes.

Also, the researcher, having identified the types of security breaches of the databases in UMYUK, a follow up question was asked to determine the extent to which cryptography prevented the occurrence of such security breaches in the databases of UMYUK. In order to achieve this objective, the opinions of the respondents were rated using five Points Likert Scale of Measurement in the following order: Very Large Extent, Large Extent, Extent, Undecided and Not at all. However, for Researcher's convenience, the options were merged into 3 to ease comprehension in the discussion as depicted in Table 4.7 below:

Table 4.7: Extent of Cryptography Prevention of Security Breaches of Databases in UMYUK

Types of Security Breaches	Extent		Undecided		Not All	
	Freq.	%	Freq.	%	Freq.	%
Viruses	8	40.0	5	25.0	7	35.0
Spyware	10	50.0	5	25.0	5	25.0
Denial of Service (DOS) Attack	5	25.0	4	20.0	11	55.0
Distributed Denial of Service (DDOS) Attack	5	25.0	5	25.0	10	50.0
Buffer Overflow Attacks	6	30.0	5	25.0	9	45.0
Brute Force Attacks	5	25.0	3	15.0	12	60.0
SQL Injection	3	15.0	2	10.0	15	75.0
Backup Data Exposure	3	15.0	2	10.0	15	75.0
Database Platform Vulnerabilities	6	30.0	3	15.0	11	55.0
Unauthorized Data Observation	10	50.0	5	25.0	5	25.0
Incorrect Data Modification	12	60.0	6	30.0	2	10.0
Phishing Scams	10	50.0	4	20.0	5	25.0
Social Engineering	6	30.0	3	15.0	11	55.0
Super-Users with Broad Access Rights	5	25.0	3	15.0	11	55.0

Table 4.7 above has depicted the responses of the respondents on the extent to which cryptography prevented security breaches in databases in UMYUK. An observation of the Table revealed that majority of the respondents with the highest frequencies of over 50% average scores respectively indicated that cryptography has not prevented the occurrences of denial of service attacks (DOS), brute force attacks, SQL injection, back up data exposure, database platform vulnerabilities,

social engineering and super users with broad access rights in the databases of Umaru Musa Yar'adua University, Katsina.

The implication of this finding is that these attacks might serve as an open invitation to exploit the vulnerabilities and breach the University's database system.

However, it can be seen that incorrect data modification 12 (60.0%), Spyware, unauthorized data observation and phishing scams with 10 (50.0%) scores each were the major security breaches that cryptography has prevented to a very large extent in Umaru Musa Yar'adua University, Katsina. This finding is in sharp agreement with the view of Steve (2007) who asserts that cryptography is used to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage in an organization. Also, the finding is in line with Schneier (1997) who posited that cryptography is so important for preventing security breach of data. Even if an intruder could gain access to institutions' network or even mobile device containing sensitive data, the data would be unreadable unless they also had access to the encryption key that unscrambles the data.

However, 25.0% of the same respondents were undecided about the extent to which cryptography prevented the occurrence of virus, spyware, distributed denial of service attack, buffer overflow attack and unauthorized data observation respectively.

4.3.4 Challenges Encountered in the Application of Cryptography in Umaru Musa Yar'adua University, Katsina

This research question was raised to identify the challenges encountered in the application of cryptography in UMYUK. In order to do this, a list of options

containing different challenges in the application of cryptography was provided for the respondents to tick as many challenges as applicable. Table 4.8 below provided a summary of the responses of the respondents:

Table 4.8: Challenges Encountered in the Application of Cryptography in UMYUK

	Yes		No	
Challenges in the Application of Cryptography	**Freq.**	**%**	**Freq.**	**%**
Poorly Designed User Interface	16	80.0	4	20.0
Quality of Encryption (sufficiently reviewed by experts)	17	85.0	3	15.0
Scalable Cryptographic Primitives	6	30.0	14	70.0
Management of the Persistent Encryption Key	5	25.0	15	75.0
Denial of Service Attacks	14	70.0	6	30.0
Encryption Can Often be a Computationally Intensive Process	16	80.0	4	20.0
Compliance Requirements and Auditors	11	55.0	9	45.0
Randomness	14	70.0	6	30.0
Use of Bad Random-Number Generator	11	55.0	9	45.0
Lack of Checking for Error Conditions Leave Secret Information in Swap Files	15	75.0	5	25.0
Speed of Encryption	18	90.0	2	10.0

Table 4.8 above has revealed that a number of challenges had affected the application of cryptography in databases in Umaru Musa Yar'adua University Katsina (UMYUK). A cursory look at the Table indicated that poorly designed user interface, quality of encryption, denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions and speed of encryption

were the common challenges encountered in the application of cryptography with the highest frequencies of over 65% response scores respectively in UMYUK. This finding was supported by Schneier (1997) who remarked that data security and the challenges of data protection are increasing in scope and difficulty. Some inherent challenges to application of cryptography in most organization include: Poorly designed user interface, speed of encryption, quality of encryption (sufficiently reviewed by experts), strength of encryption (algorithm, key size), denial of service attacks and lack of checking for error conditions leave secret information in swap files.

On the other hand, it was revealed that scalable cryptographic primitives and management of the persistent encryption key were the only 2 challenges not encountered in the application of cryptography with the highest frequencies of over 65% response scores.

Also, having identified the challenges encountered in the application of cryptography in UMYUK, a follow up question was asked to determine the extent of the challenges encountered in the application of cryptography in Umaru Musa Yar'adua University. This is necessary because organizations need to think beyond the traditional models of securing the perimeter and locking down specific segments of IT infrastructure in order to formulate their data protection goals. To realize this objective, Five Points Likert Scale of Measurement was used in this order: Very Large Extent, Large Extent, Undecided, Extent and Not at all. However, for Researcher's convenience, the options were merged into 3 to ease comprehension in the discussion as shown in Table 4.9 below:

Table 4.9: Extent of Challenges Encountered in the Application of Cryptography in UMYUK

Challenges in the Application of Cryptography	Extent		Undecided		Not all	
	Freq.	%	Freq.	%	Freq.	%
Poorly Designed User Interface	11	55	5	25.0	4	20.0
Quality of Encryption (sufficiently reviewed by experts)	13	65.0	4	20.0	3	15.0
Scalable Cryptographic Primitives	5	25.0	1	5.0	14	70.0
Management of the Persistent Encryption Key	20	100.0	0	0	0	0
Denial of Service Attacks	5	25.0	1	5.0	14	70.0
Encryption Can Often Be a Computationally Intensive Process	12	60.0	4	20.0	4	20.0
Compliance Requirements and Auditors	7	35.0	4	20.0	9	45.0
Randomness	11	55.0	3	15.0	6	30.0
Use of Bad Random-Number Generator	8	40.0	3	15.0	9	45.0
Lack of Checking For Error Conditions Leave Secret Information in Swap Files	10	50.0	5	25.0	5	25.0
Speed of Encryption	13	65.0	5	25.0	2	10.0

Table 4.9 above has shown that management of persistent encryption key, speed of encryption, computationally nature of cryptography and quality of encryption (sufficiently reviewed by experts) were the challenges encountered in the application of cryptography in Umaru Musa Yar'adua University, Katsina, with the highest frequencies of over 60% response scores respectively. This is followed by denial of service attacks, poorly designed user interface and randomness with the frequencies of over 50% response scores each respectively.

Also, it was found that scalable cryptographic primitives14 (70.0%) was not affected the implementation of cryptography in the University studied at all. This is followed by compliance requirements and auditors and use of bad random number generator with 9 (45%) response scores each respectively.

However, it was surprising to find that less than 30% of the respondents were undecided about the levels of difficulties of the challenges encountered in the application of cryptography in Umaru Musa Yar'adua University, Katsina.

This finding showed that those responsible for the database management in UMYUK are either not qualified or the Network Security Engineer and Systems Engineer are not included in the DICT. Schneier (1997) posited that design work is the mainstay of the science of cryptography, and it's very specialized. Cryptography blends several areas of mathematics: number theory, complexity theory, information theory, probability theory, abstract algebra, and formal analysis. Few can do the science properly, and a little knowledge is a dangerous thing: Inexperienced cryptographers almost always design flawed systems. Nothing substitutes for extensive peer review and years of analysis

4.4 Inferential Analysis

This section deals with the outcome of inferential analysis employed to test the null hypotheses formulated for this study. The research used 0.05 as the level of significance for testing the hypotheses. This is because behavioural science researches involve human beings and the 0.05 level of significance is generally accepted. Null hypothesis one was tested using Pearson Product Moment Correlation Co-efficient and null hypothesis two was tested using Chi-Square, all at 0.05 level of significance. The findings were presented as follows:

4.4.1 Null Hypothesis One

There is no significant relationship between database accessibility and the types of security threats they are exposed to in Umaru Musa Yar'adua University, Katsina.

Table 4.10: Correlation Between the Types of Databases Accessibility and the Types of Security Threats They Are Exposed to in UMYUK

Variables	N	Mean	Std. Dev.	Std. Error	r-calc.	DF	P	Remark
Database access	20	3.0167	.32699	.07312	0.039	18	0.869	NS
Database threats	20	7.5500	2.11449	.47281				

The above Table 4.10 was subjected to Pearson Product Moment Correlation Coefficient (PPMC). The calculated r-value of 0.039 at the degree of freedom of 18 and α 0.05 level of significance was obtained. The calculated r-value of 0.039 is less than the table value of 0.444 at the same degree of freedom and confidence level as the observed significance level of 0.869 is greater than 0.05. The null hypothesis which says there is no significant relationship between database accessibility and the types of security threats they are exposed to in Umaru Musa Yar'adua University, Katsina is therefore retained.

This implies that the databases accessibility is not significantly related to the type of security threat the databases are exposed to in the University studied.

4.4.2 Null Hypothesis Two

H_{o2}: Application of cryptography has no significant effect on the prevention of security breach of databases in Umaru Musa Yar'adua University, Katsina.

Table 4.11 Significant Effect of Cryptographic Prevention to Security Breaches of Databases in UMYUK

Security Breaches	Significantly Affected	Affected	Undecided	Fairly Affected	Not Affected	Total
Viruses	0(3.0)	4(1.40)	5(2.40)	4(2.20)	7(13.70)	20
Spyware	0(3.0)	4(1.40)	5(2.40)	6(2.40)	5(13.70)	20
Denial of Service (DOS) Attack	0(3.0)	1(1.40)	4(2.40)	4(2.40)	11(13.70)	20
Distributed Denial of Service (DDOS) Attack	0(3.0)	1(1.40)	5(2.40)	4(2.40)	10(13.70)	20
Buffer Overflow Attacks	0(3.0)	0(1.40)	5(2.40)	6(2.40)	9(13.70)	20
Brute Force Attacks	0(3.0)	1(1.40)	3(2.40)	4(2.40)	12(13.70)	20
SQL Injection	1(3.0)	2(1.40)	2(2.40)	0(2.40)	15(13.70)	20
Backup Data Exposure	0(3.0)	1(1.40)	2(2.40)	2(2.40)	15(13.70)	20
Database Platform Vulnerabilities	0(3.0)	2(1.40)	3(2.40)	4(2.40)	1(13.70)	20
Unauthorized Data Observation	0(3.0)	1(1.40)	5(2.40)	9(2.40)	5(13.70)	20
Incorrect Data Modification	0(3.0)	2(1.40)	6(2.40)	10(2.40)	2(13.70)	20
Phishing Scams	0(3.0)	3(1.40)	4(2.40)	7(2.40)	5(13.70)	20
Social Engineering	0(3.0)	2(1.40)	3(2.40)	4(2.40)	11(13.70)	20
Super-Users with Broad Access Rights	0(3.0)	3(1.40)	3(2.40)	2(2.40)	11(13.70)	20
Total	1	27	53	62	119	280

Chi-Square = 95.940, DF = 52, P0.072

Expected counts are printed in bracket along observed counts.

From Table 4.11, the X^2 calculated is 95.940 at α = 0.05, degree of freedom (DF) 52 and the P value is 0.072. This showed that p value of 0.072 is greater than α 0.05. Hence the null hypothesis which says application of cryptography has no significant effect on the prevention of security breach of electronic databases in Umaru Musa Yar'adua University, Katsina is therefore retained.

References

Schneier, B. (1997). Cryptography, Security and the Future. Retrieved 10th April, 2014. From http://www/schnnier.com/cryptography.html.

Symantec (2009). Anatomy of a Data Breach: Why Breaches Happen and What to Do about It. USA :Symantec World Headquarters 350 Ellis St. Mountain View.

Steve G. (2007). Databases for Embedded Systems. *Embedded Computing Design* magazine. Retrieved on August 13, 2013 from http//www.embedded-computing.com

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter provides the summaries of the study, conclusion and recommendations based on the research findings. The chapter also advanced some suggestions for further research.

5.2 Summary of the Study

The purpose of this study was to investigate the Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina. In order to achieve this objective, four research questions were formulated and two null hypotheses were tested. A survey research method was employed in carrying out the study. The population of the study comprised all the staff of the Directorate of Information and Communication Technology in Umaru Musa Yar'adua University, Katsina. Due to the fact that the population is not too large, all the 21 staff were used as sample for this study. Hence no sampling technique was applied. Questionnaire and observation were the instruments used for data collection in this study. In collecting the data, a research assistant was used to facilitate the exercise.

The data collected were analysed and presented using descriptive statistics such as frequency distribution tables and percentages. Also, inferential statistics was employed to test the hypotheses formulated for the study. The null hypothesis one was tested using Pearson Product Moment Correlation Co-efficient and null hypothesis two was tested using Chi-Square all at 0.05 level of significance.

5.2 Summary of the Major Findings

Based on the data collected and analysed, the following are the major findings of the study:-

1. That personnel records database, financial records database, and students academic records database were the types of databases available with the highest frequencies of 100.0% response scores respectively in UMYUK. While, the personnel records database, financial records database, students academic records database, students hostel records database and students medical records database were the databases that were accessible with the total frequencies of over 50% response scores respectively.
2. That data tempering, password-related threats, worms, intrusion by unauthorized users, clicking unnecessary links and privilege abuse were the security threats exposed to the databases with the highest frequencies of over 60% scores respectively in Umaru Musa Yar'adua University Katsina.
3. That cryptography has not prevented the occurrences of denial of service attacks (DOS), brute force attacks, SQL injection, backup data exposure, database platform vulnerabilities, social engineering and super users with broad access rights with the highest frequencies of over 50% average scores respectively in UMYUK.
4. That poorly designed user interface, quality of encryption, denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions and speed of encryption were the common challenges encountered in the application of cryptography with the highest frequencies of over 65% response scores respectively in UMYUK

5. The null hypothesis which says there is no significant relationship between database accessibility and the types of security threats they are exposed to in Umaru Musa Yar'adua University, Katsina is therefore retained.
6. The null hypothesis which says application of cryptography has no significant effect on the prevention of security breach of databases in Umaru Musa Yar'adua University Katsina is therefore retained.

5.3 Conclusion

From the analysis and summary of the findings of the study, it is clear that the Directorate of Information and Communication Technology of Umaru Musa Yar'adua University, Katsina has realized the need for the application of cryptography as part of defense-in-depth strategy for providing reasonable protection of sensitive information vis-à-vis the means of detection and remediation of security breaches. However, the DICT does not explore, to a large extent, the advantages of security mechanisms opened in the application of cryptography for preventing the occurrences of most security breaches on the databases of the University, which include the denial of service attacks (DOS), brute force attacks, SQL injection, back up data exposure, database platform vulnerabilities, social engineering and super users with broad access rights. This paved way for cyber-crimes. When security safeguards are not adequate, trespassers run little risk of getting caught. They can attack a system using techniques the designers never even considered. Hence, the need for constant improvement in securing the vital information. Hence, it can be concluded that if all the cryptographic challenges, security breaches, threats and vulnerabilities were addressed, it would enhance the effectiveness of information security and project new image as well as the perception of the University to safeguard its vital information against well-meaning

insiders, malicious insiders and targeted attacks. It would in turn encourage University managers to reward the DICT with increased resources to further enhance the necessary information security measure.

5.4 Recommendations

In line with the findings of the study, it is recommended that:

1. The University should adopt strategic information records database for keeping records of valuable assets, day-to-day operations, and executive decision-making and intellectual rights in efforts to prevent theft of institutions' secrets and confidential documents. And the user must have the necessary level of access to the database system to perform the duties within their position and should be responsible for the following operational security procedures to ensure the university's' data confidentiality, integrity, and availability.
2. Information security risk assessment and management should be made an integral component of DICT policy document. This will go a long way in preventing and minimizing the threat level of data by intruders and other malicious attacks in the University's databases. This is a prerequisite for the University to successfully survive and compete in the 21st Century.
3. The Directorate of Information and Communication Technology should as a matter of policy, mount a regular training programme such as seminars, workshops, symposia and in-house IT training for their staff in order to equip them with the latest development in the areas of information security systems so as to provide means of detection and remediation of security breaches of databases such as phishing scams and the like.

4. The need for employment of specialist in the areas of Information Security for safeguarding vital information in the Directorate of Information and Communication Technology is highly advocated as it would help the DICT staff to identify gaps that need to be closed in terms of challenges hindering the application of cryptography in UMYUK to cater for the database security breaches. A number of specific challenges confronting UMYUK in the application of cryptography were identified in the study which include: poorly designed user interface, quality of encryption, denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions and speed of encryption. The aforementioned must be implemented perfectly or the system will fail. It is therefore, necessary for the DICT staff to understand the trust relationships between different entities involved in a cryptographic protocols so as to improve the current situation (Information Security) in the University. And above all, encryption should not only be used but constantly reviewed by peers to face the threat of a growing society.

5.5 Suggestion for Further Research

In the light of the findings and conclusions of the study, further researches in the following areas are suggested:

1. Design and Implementation of Visual Cryptography for Protection against Phishing Scams Threats in the Universities in Northern States of Nigeria.
2. Content Management Strategies in Universities' Website in North-West Geopolitical Zone of Nigeria.
3. Management of Staff and Students' information in the Universities in Six Geo-Political Zones of Nigeria.

Bibliography

Abomhara, M. (2011). Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard. MSc. Thesis: University of Malaya.

Adedokun, O. M and Ejeh, U.L. (2010). Instruction to Research Method in Geography and Social Sciences. Kaduna: Esonaj Ent. Nig. Ltd.

Adekeye, W.U (1997). *The Importance of Management Information Systems.* Ilorin: University of Ilorin.

Aliyu, A. (2011). Information Anxiety Among Internet Users in Ahmadu Bello University, Zaria**.** Unpublished MLS Thesis Work. A.B.U University, Nigeria.

Anley C. (2002). Advanced SQL Injection in SQL Server Applications. White Paper, Next Generation Security Software Ltd. London.

Bagdanov, D. (2007). How to Securely Perform Computation on Secret Shared Data. MSc. Thesis: University of Tartu.

Basden, A. (2010). On Using Spheres of Meaning to Define and Dignify the IS Discipline. *International Journal of Information Management*, 30, 13-20.

Benbasat, I. (1980). The Case Research Strategy in Studies in Information System. Retrieved on 26th April, 2014. From http:// www.coba.usf.edu/departments.

Bernard , J. (2012). Perfecting Your Research Work. London, Unique Press.

Binjo (2012). Cyber-Crime, Education. Retrieved on 2nd November, 2014 from http:// www.technsstivity.com/category/education/

Bolton, D. (2013). *Definition of Encryption*. Retrieved 3rd May, 2013 from cplus.about.com/od/glossal1/g/algoriyhm.htm.

Buaki, J. (2013). Information System Security Best Practice. Retrieved 5 May, 2013 from http//www.about.com.

Chaudhuri, S., Narasayya, V., (1997). An Efficient, Cost-Driver Index Selection Tool for Microsoft SQL Server," *Proceedings of the 23rd VLDB Conference*, Athens, Greece.

Christian Kirsch –Thales (2009). The Role of Encryption in Database Security. Retrieved 14th January, 2014 from http://www.net-security.org/insecure-archive.php.

Creswell, J. W. (2003). Research Design, Quantitative, Qualitative and Mixed Method Approaches. California: Sage Publications, Inc.

David, K. (2004). Effective Oracle Database 10g Security: London: McGraw-Hill.

Ekeh, F. I. (2003). Research Methodology and Statistics in Education. Nsukka: Madol Press. pp72-88.

Elsevier, B.V. (2014). Database Systems: Challenges and Opportunities For Graphical HCI. Retrieved April, 2014. From http://www/.elsvier.com/.

Granger (2001). Social Engineering Fundamental, Part 1: Hacker Tactics.

Galbreath, N. (2003). Cryptography for Internet and Database Applications: Developing Secret and Public Key Techniques with Java, Retrieved 15h January, 2014 from http://eu.wiley.com/WileyCDA/Section/id-302479.html?query=Nick+Galbreath.

Harris, S. (2007). CISSP® All-in-One Exam Guide. McGraw-Hill.

Ibikunle, F. (2013). *Approach to Cyber Security Issues In Nigeria*. Retrieved 2nd November, 2014, from *http://ijcrsee.com/index.php/ijcrsee/article/view/11/114*

Isangedighi, A. J. and Ogomaka, M.C. (1992). Education Research Methods. Totan publishers Limited, Abuja-Nigeria

Issam , M. (2010). Efficient Hardware Implementations for the Advanced Encryption Standard (AES) Algorithm. MSc. Thesis Dalhousie University Halifax, Nova Scotia.

Jarvinen, K. (2008). Studies on Efficient Implementation of Cryptographic Algorithms. A Thesis For the Degree of Doctor of Science in Technology, Helsinki University of Technology.

Jen, S. U. (2002). Fundamentals of Research Methodology. Yola: Paraclete Publishers. pp75-81

Jessup, Leonard M. Joseph S. Valacich (2008). *Information Systems Today* (3rd ed.). Pearson Publishing. Glossary p. 416.

John, W., and Joe, P. (2002). Strategic Planning for Information System. 3rd Ed. West Sussex. John Wiley & Sons Ltd.

Justin, M. and Manimurugan, S. (2012). Survey on Various Encryption Techniques, *International Journal of Soft Computing and Engineering* .ISSN: 2231-2307, Volume-2, Issue-1

Kabay, M. (2004). *What's Important for Information Security*. Retrieved 11, May, 2013 from http://www.mekabay.com/overviews/infosec_ed.htm .

Katz, J. and Lindell, Y (2007). Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall/CRC , Boca Raton London New York.

Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. M.G.M's College of Engineering and Technology, Navi Mumbai, India

Kenan, K. (2005). Cryptography in the Database: The Last Line of Defense. Retrieved July, 2013, from Http://www.awprofessional/bookstore/product.asp

Kessler, G. (2013). *An Overview of Cryptography*. Retrieved 8th May, 2013 from http://www.garykessler.net/kumquat_pubkey.html.

Kimmo, J. (2008). Studies on Efficient Implementation of Cryptographic Algorithms. PhD. Dissertation Helsinki University of Technology.

Kioskea (2013). Introduction to Information Technology Security. Retrieved on May, 2013. From http://www.facebook.com/pages/Kioskea/117422445065179.

Kremlin (2008). Concept of Cryptography. Retrieved 12th April, 2014. From http://www.kremlinencrypt.com/concepts.htm

Lisa, W. (2009). Fast Flexible Architectures for Secure Communication. MSc. Thesis, University of Michigan.

Maurer, U. (2004). The Role of Cryptography in Database Security. Zurich, Switzerland: Springer.

Mahmud, S. (2004). A Study on Parallel Implementation of Advanced Encryption Standard (AES). M.Sc Thesis in Independent University, Bangladesh.

Menezes, A.J. Van Oorschot, P.C. And Vanstone, S.A. (1997). *Handbook of Applied Cryptography*. London: CRC Press.

Miessler, D. (2013). An Information Security Concepts Primer. Retrieved on 9th May, 2013. From http//creativecommon.org.

Mohammed, Z. (2003). A Study of the Status of ICT Availability and Applications in Nigerian Libraries and Information Centres. A paper presentation at A.B.U.Zaria.

Mohammed, Z. (2009). Capacity Building for Library and Information Centre Personnel in ICT Environment. Ahmadu Bello University, Zaria. *pp.9-13*.

Mohammed, Z. (2012). Fifty Years of Library and Information Service in Ahmadu Bello University, Zaria. *A Paper Presented at the Symposium to Mark the Ahmadu Bello University, Zaria 50th Anniversary Golden Jubilee Celebrations.*

McCurley, K. S. (1996). Cryptography and the Internet: Lessons and Challenges. Retrieved 24th March, 2014 from http://www.mccurley.org/papers/asiacrypt96/

Murphy. S and Badger, M. (1996). ``Digital Signature Protection of the OSPF Routing Protocol", Proceedings of the 1996 Symposium on Network and Distributed Systems Security, IEEE,

Nairaland (2014). A.B.U Zaria 2014/2015 Admission Thread – Education. Retrieved 2nd November, 2014 from *www.nairaland.com/1582985/a.b.u-zaria-2014-2015-admission/40*

NGScholars (2014)· ASUU Strike: Bayero University Website Hacked. Retrieved 2nd November, 2014 from http: // *www.ngscholars.com*/category/

Office of Information Technology (2012). Definition of Information Security. Las Vegas, University of Nevada. Retrieved on 18th April, 2013 from *http://oit.unlv.edu/network-and-security*.

Omotosho, A. (1991). Statistics Method. Ibadan: N.P.S. Educational Publishers Ltd.

Osuala, E. C. (2005). Introduction to Research Methodology. Nimo: Rex Charles and Patrick. pp253-267.

Paar,C. Pelzl, J. (2010). *Understanding Cryptography*, Springer-Verlag Berlin Heidelberg .

Pawlan, M. (1998). Cryptography: The Ancient Art of Secret Messages. Retrieved May 4, 2013, from http://www.pawlan.com/Monica/crypto/

Pell, O. (2013). A brief History of Cryptography and Cryptology. Retrieved 0n 8th May, 2013 from http:// www. Doc.ic.uk.

Radhakrishna, R.B. (2007). Tips For Developing and Testing Questionnaires/Instruments. Journal of Extension. Vol. 45 no. 1 pp. 1-4. (E J). Ltd.

Ramakrishnan, P. (2003). Information Security Management Systems. Retrieved on 13 May, 2013frommhtml:file://E:\Whitepaper\Information%20Security%20Management%20Systems.mh.

Richardson, R. (2008). CSI Computer Crime and Security Survey. California, Irvine.

Rodriguez, G. (2014). What are the Most Common Types of Databases. Retrieved on 14TH January, 2014 from http://www.life123.com/author/gene_rodriguez,_iii.

Ronald, L. (1990). *Handbook of Theoretical Computer Science* 1. Elsevier.

Rouse, M. (2007). *Security Policy*. Retrieved 9th May, 2013 from http://whatis.techtarget.com/contributor/Margaret-Rouse

Rouse. M (2007) Definition of Phishing. Retrieved on 15th April, 2014. From http://searchsecurity.techtarget.com/definition/phishing

Rubin, J. (2008). Vigenere Cipher. Retrieved May 4, 2013, from http://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html.

Ruskwig (2011). Security Policies. Retrieved 10th May, 2013, from http://www.ruskwig.com/it security policy.htm.

SafeNet (2014). Data Encryption Solutions. Retrieved 24th March, 2014, from http://www.securethebreach.com/

Safety and Security Centre (2014). How to Recognize Phishing Email Messages, Links, or Phone Calls. Retrieved on 15th April, 2014. From http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx.

Sambo, A.A. (2008). Research Methods in Education. Lagos: Sterling Hoden Publishers (Nig) Ltd. Pp 341-354.

Savu, L. (2013). *Cryptography Role in Information Security*. Romania: University of Bucharest,

Schneier, B. (1996). Applied Cryptography. New York: Wiley.

Schneier, B. (1997). Cryptography, Security and the Future. Retrieved 10th April, 2014. From http://www/schnnier.com/cryptography.html.

Schneider, L. (2013). Information Security - Learn about Information Security. Retrieved on 18th April, 2013 from *http://www.about.com/*.

Simpson, S. (1997). Cryptography in Everyday Life. Retrieved 6th May, 2013 from www.laist.com.edu.

Stallings, W. (2003). Cryptography and Network Security, Principles and Practices. Third Edition. USA: Pearson Education, Inc.

Steve G. (2007). Databases for Embedded Systems. *Embedded Computing Design* magazine. Retrieved on August 13, 2013 from http//www.embedded-computing.com

Symantec (2009). Anatomy of a Data Breach: Why Breaches Happen and What to Do about It. USA: Symantec World Headquarters 350 Ellis St. Mountain View.

Sudarshan, K.S. (2001). Database System Concepts, Fourth Edition, McGraw−Hill Companies.

Sveiby, K.E. (1994). *What is Information*. Retrieved 12th April, 2014. From http://www.sveiby.com/articles/polanyi.html

Taylor, K. (2002). Number Theory 1. Retrieved May 4, 2013, from http://math.usask.ca/encryption/lessons/lesson00/page1.html.

Techterm.com (2013). *Definition of cryptography*. Retrieved May 3rd, 2013, from www.techterms.com/category/technical.

TechTarget (2011). Encryption techniques and products for hardware-based data storage security. Retrieved 8 may, 2013 from http://www.computerweekly.com/about/copyright.

Thomas, R. (1996). Survey in Research Methods: Guide for postgraduate Studies (ed) By Tony Greenfield, London: Arnold.

Umaru Musa Yar'adua University, Katsina Official Website: http://www.umyu.edu.ng (n.d.)

United Kingdom Essays (2013). Database Security and Encryption. Retrieved 5th July, http://www.ukessays.com/

Wayne, M. (1998). *Cryptography and Liberty*. Retrieved from http://www.gilc.org/ on 3rd May, Security+ Certification: Exam Guide. McGraw-Hill.

Whitman, M. and Mattord, H. (2005). *Principles of Information Security*. University of Phoenix Custom Edition e-text. Canada, Thomson Learning, Inc. Retrieved May 4th, 2013, from University of Phoenix, rEsource, CMGT/432.

APPENDIX I

Database Encryption System

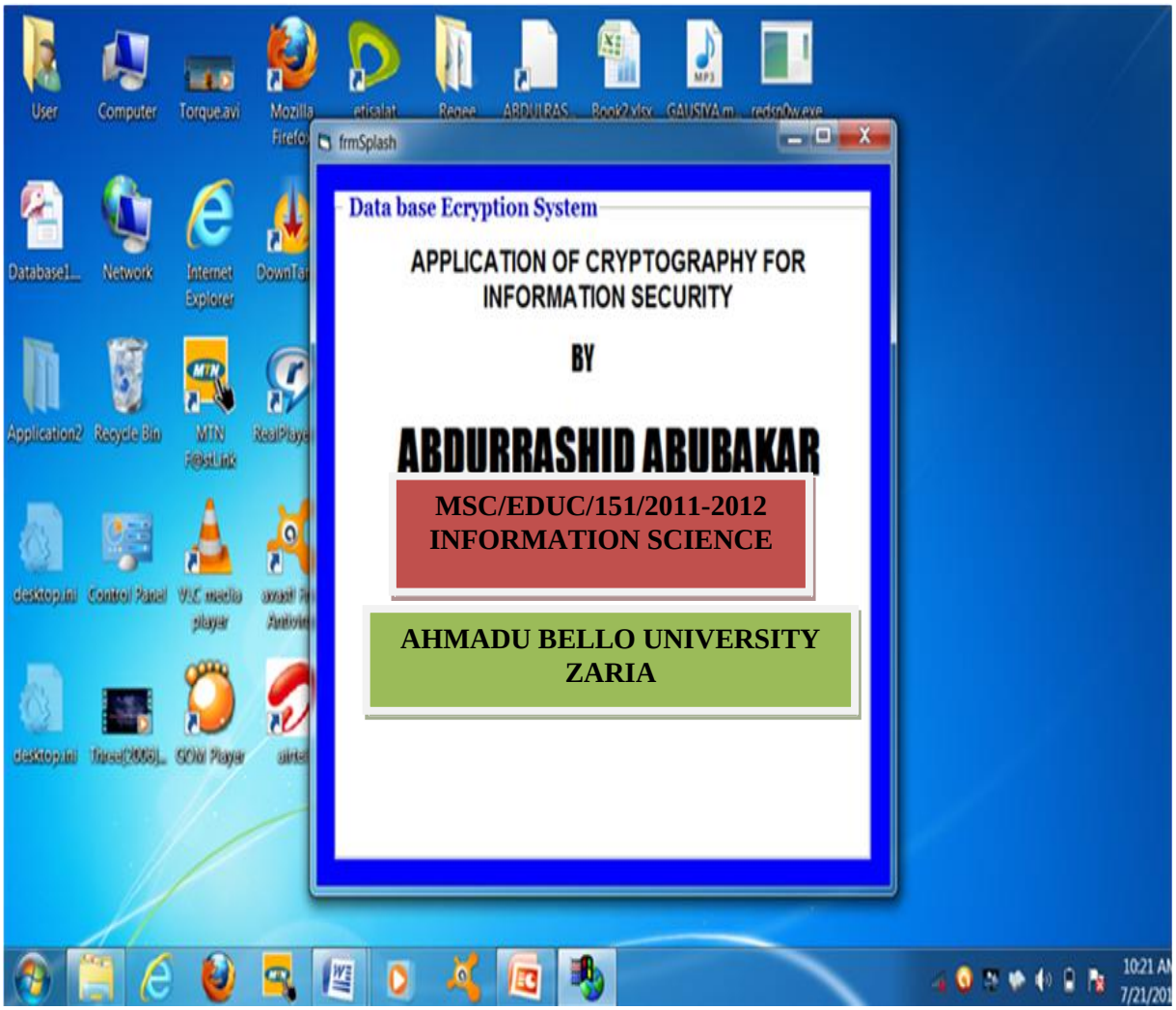


Figure 5.1: Database Encryption System Interface

Figure 5.2: Login Form For Authorized User

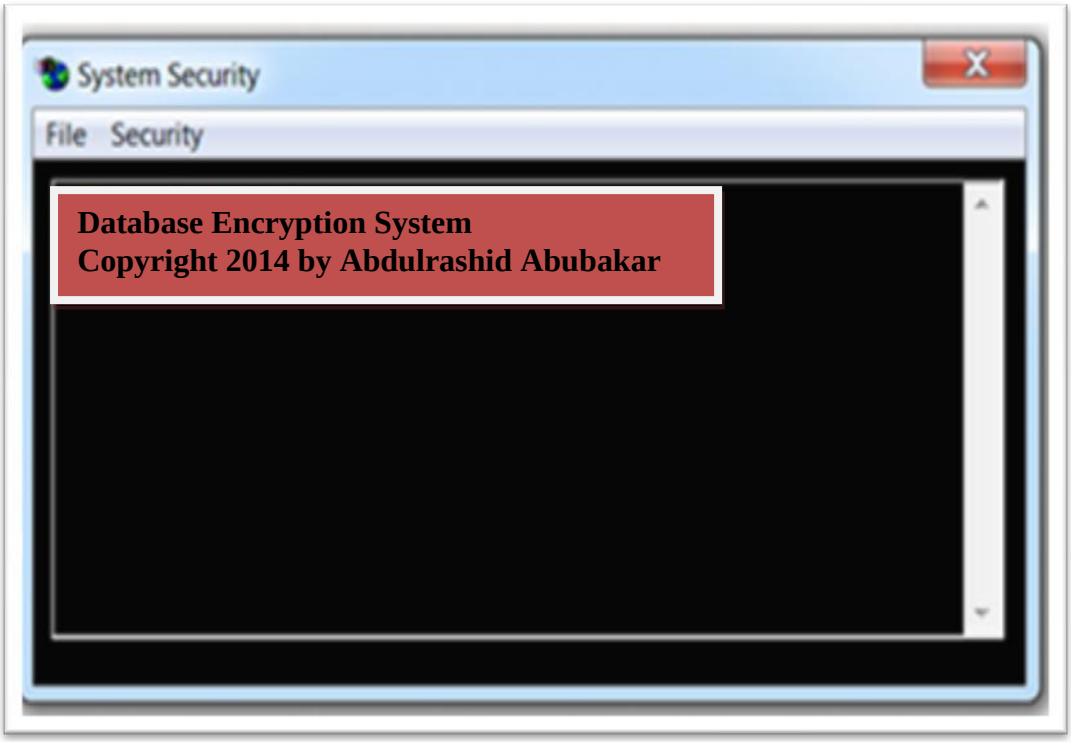


Figure 5.3: User Interface

Figure 5.4: Drop Down Menu For File and Database Encryption

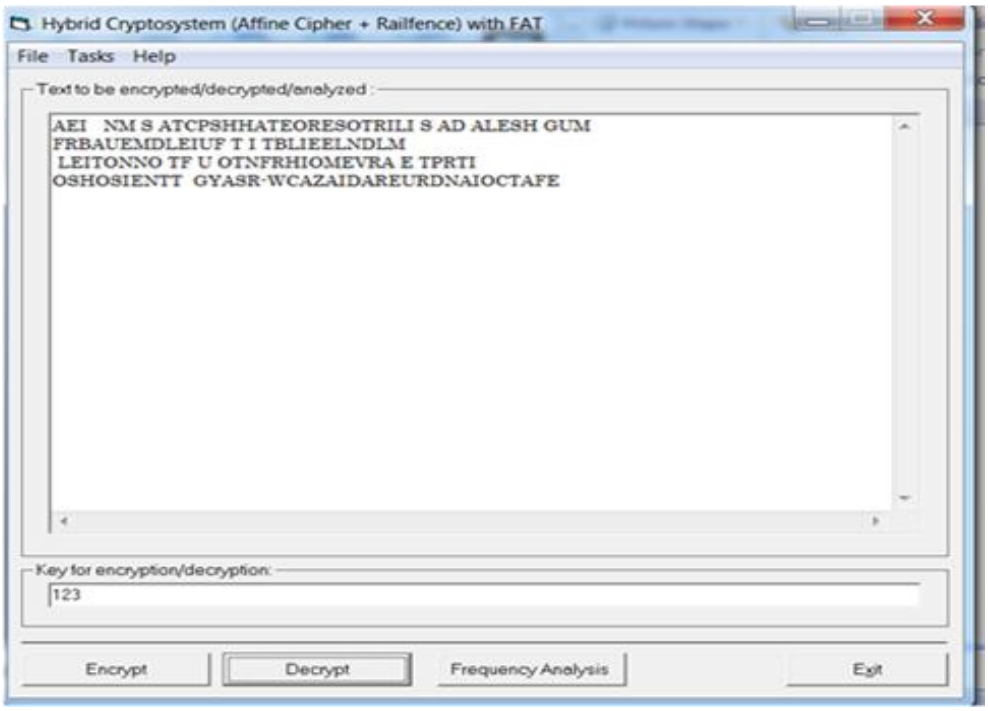


Figure 5.5: Sample Encrypted Text

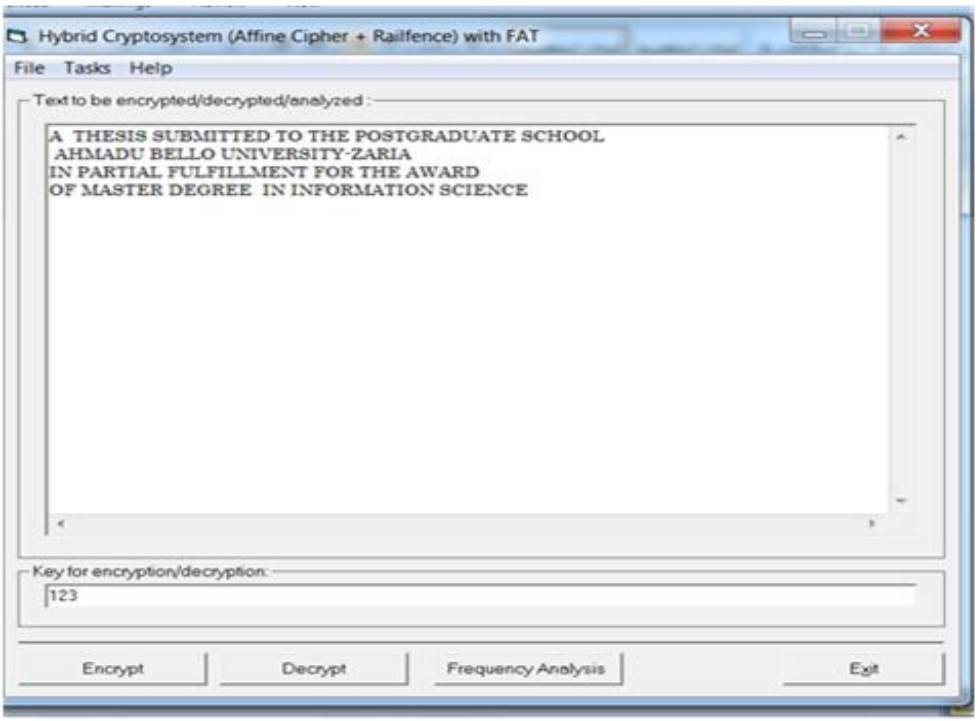


Figure 5.6: Decrypted Text

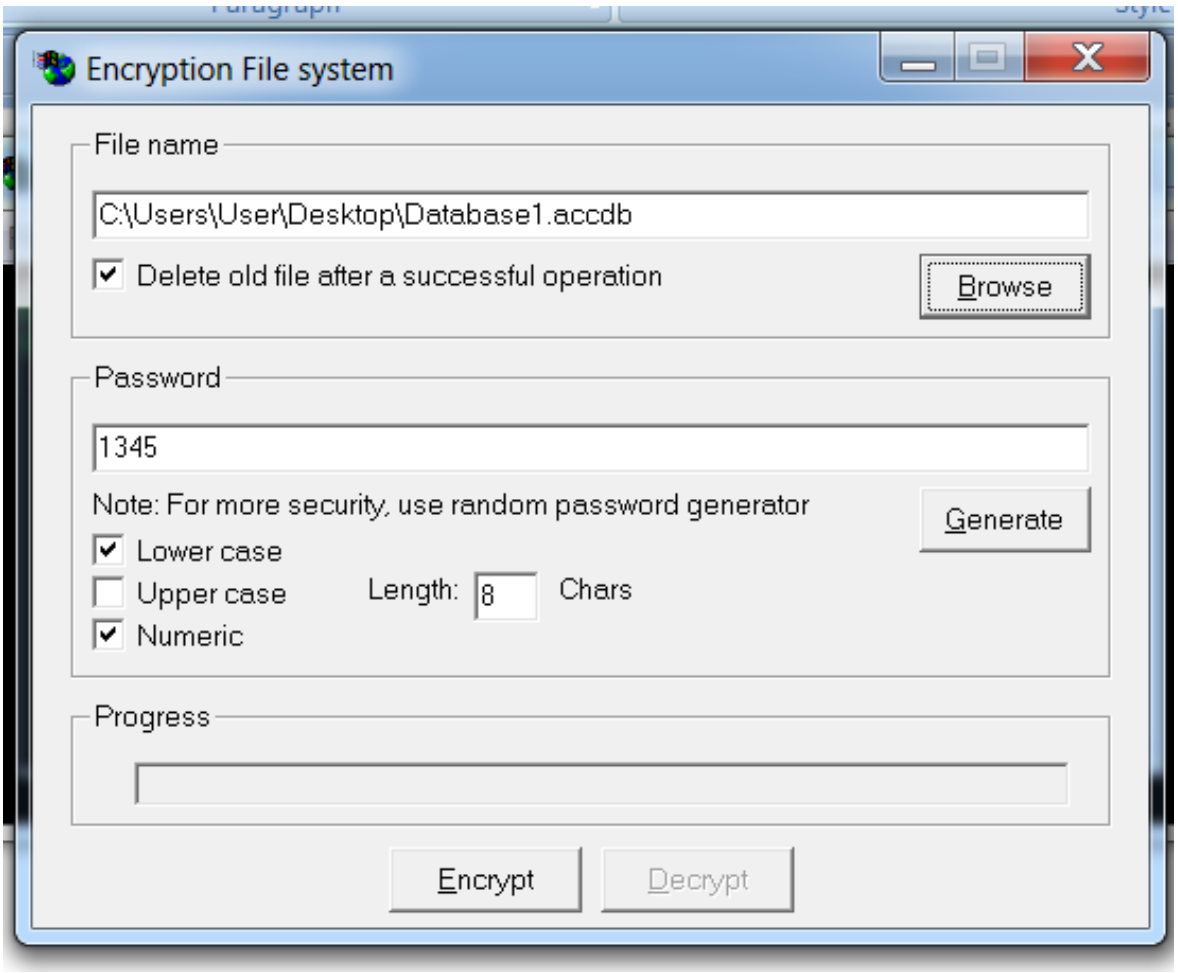


Figure 5.7: Database Encryption

APPENDIX II

Questionnaire for Directorate of Information and Communication Technology Staff

Department of Library and Information Science,
Faculty of Education,
Ahmadu Bello University, Zaria.

Date: 22nd April, 2014.

Dear Respondent,

REQUEST TO FILL QUESTIONNAIRE ON APPLICATION OF CRYPTOGRAPHY FOR INFORMATION SECURITY IN UMARU MUSA YAR'ADUA UNIVERSITY, KATSINA (UMYUK).

I am a Post Graduate Student of Ahmadu Bello University, Zaria, undertaking a research work entitled "Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina" for the award of MSc in Information Science. I am therefore requesting you to kindly supply answers to the questions as contained in the attached questionnaire which meant for academic research purposes. You are guaranteed of strict confidentiality of any information provided.

Your quick response will be highly appreciated.

Thank you.

Yours faithfully,

ABDULRASHID ABUBAKAR
MSC/EDUC/151/2011-2012

INSTRUCTIONS:

Please kindly fill the space provided/ tick [√] as many as applicable in the questionnaires below:

SECTION A: PERSONAL INFORMATION

(1) Department/Unit: _____

(2) Rank: ……

SECTION B: TYPES OF DATABASES AVAILABLE AND ACCESSIBLE

(3) What types of databases are available in UMYUK?

(a)	Personnel Records Database	[ ]
(b)	Financial Records Database	[ ]
(c)	Strategic Information Records Database	[ ]
(d)	Students Hostels Records Database	[ ]
(e)	Student Academic Records Database	[ ]
(f)	Medical Records Database	[ ]
(g)	Others (Please specify)_____	

(4) How accessible are the databases in UMYUK?

S/N	Types of Databases Accessible	Highly Accessible	Accessible	Undecided	Fairly Accessible	Not Accessible
1	Personnel Records Database					
2	Financial Records Database					
3	Strategic Information Records Database					
4	Students Hostels Records Database					
5	Students Academic Records Database					
6	Medical Records Database					
7	Others (Please Specify)					

SECTION C: SECURITY THREATS TO DATABASES

(5) What types of security threats are databases in UMYUK exposed to?

(a)	Data Tampering	[ ]
(b)	Password-Related Threats	[ ]
(c)	Worms	[ ]
(d)	Intrusion by Unauthorized Users	[ ]
(e)	User Ignorance of the System's Functionalities	[ ]
(f)	Lack of knowledge of the security measures in place	[ ]
(g)	Improper Input Validation	[ ]
(h)	Violating the IT Security Policy	[ ]
(i)	Clicking Unnecessary Links	[ ]
(j)	Privilege Abuse	[ ]
(k)	Legitimate Privilege Abuse	[ ]
(l)	Privilege Promotion	[ ]
(m)	Operating System Vulnerabilities	[ ]
(n)	Others (Please Specify)……..	

(6) Please indicate the level of security threats that databases are exposed to in UMYUK

S/N	Security Threats	Highly Exposed	Exposed	Undecided	Fairly Exposed	Not Exposed
1	Data Tampering					
2	Password-Related Threats					
3	Worms					
4	Intrusion by Unauthorized Users					
5	Lack of knowledge of the security measures in place					
6	User Ignorance of the System's Functionalities					
7	Improper Input Validation					
8	Violating the IT Security Policy					
9	Clicking Unnecessary Links					
10	Privilege Abuse					
11	Legitimate Privilege Abuse					
12	Privilege Promotion					
13	Operating System Vulnerabilities					
14	Others (Please specify)					

SECTION E: EXTENT OF CRYPTOGRAPHY PREVENTION OF SECURITY BREACH IN DATABASES

(7) Which of the following security breaches has databases experienced in UMYUK?

(a)	Viruses	[ ]
(b)	Spyware	[ ]
(c)	Denial of Service (DOS) Attack	[ ]
(d)	Distributed Denial of Service (DSDOS) Attack	[ ]
(e)	Buffer Overflow Attacks	[ ]
(f)	Brute Force Attacks	[ ]
(g)	SQL Injection	[ ]
(h)	Backup Data Exposure	[ ]
(i)	Database Platform Vulnerabilities	[ ]
(j)	Unauthorized Data Observation	[ ]
(k)	Incorrect Data Modification	[ ]
(l)	Phishing Scams	[ ]
(m)	Social Engineering	[ ]
(n)	Super-Users with Broad Access Rights	[ ]
(o)	Others (Please Specify)…….....	

(8) To what extent has cryptography prevented the security breach of databases in UMYUK?

S/N	Types of Security Breaches Experienced in Databases	Very Large Extent	Large Extent	Undecided	Extent	Not at All
1	Viruses					
2	Spyware					
3	Denial of Service (DOS) Attack					
4	Distributed Denial of Service (DDOS) Attack					
5	Buffer Overflow Attacks					
6	Brute Force Attacks					
7	SQL Injection					
8	Backup Data Exposure					
9	Database Platform Vulnerabilities					
10	Unauthorized Data Observation					
11	Incorrect Data Modification					
12	Phishing Scams					
13	Social Engineering					
14	Super-Users with Broad Access Rights					
15	Others (Please Specify)					

SECTION F: CHALLENGES ENCOUNTERED IN THE APPLICATION OF CRYPTOGRAPHY

(9) What are the challenges encountered in the Application of Cryptography in UMYUK?

(a) Poorly Designed User Interface [ ]

(b) Quality of Encryption (sufficiently reviewed by experts) [ ]

(c) Management of the Persistent Encryption Key [ ]

(d) Scalable Cryptographic Primitives [ ]

(e) Denial of Service Attacks [ ]

(f) Encryption Can Often be a Computationally Intensive Process [ ]

(g) Compliance Requirements and Auditors [ ]

(h) Randomness (Use of Random Number Generator) [ ]

(I) Under deadline and budget pressures implementers use bad random-number generator [ ]

(j) Lack of Checking For Error Conditions Leave Secret Information in Swap Files [ ]

(k) Speed of Encryption [ ]

(l) Others (please specify)……

(10) Please indicate the extent of challenges encountered in the application of cryptography in UMYUK?

S/N	Challenges in the Application of Cryptography	Very Large Extent	Large Extent	Undecided	Extent	Not at All
1	Poorly Designed User Interface					
2	Quality of Encryption (sufficiently reviewed by experts)					
3	Scalable Cryptographic Primitives					
4	Management of the Persistent Encryption Key					
5	Denial of Service Attacks					
6	Encryption Can Often be a Computationally Intensive Process					
7	Compliance Requirements and Auditors					
8	Randomness (Use of Random Number Generator)					
9	Under Deadline Implementers Use Bad Random-Number Generator					
10	Lack of Checking For Error Conditions Leave Secret Information in Swap Files					
11	Speed of Encryption					
12	Others (Please specify)					