UNIVERSITY OF JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

- NonCommercial — You may not use the material for commercial purposes.

- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

Surname, Initial(s). (2012) Title of the thesis or dissertation. PhD. (Chemistry)/ M.Sc. (Physics)/ M.A. (Philosophy)/M.Com. (Finance) etc. [Unpublished]: University of Johannesburg. Retrieved from: https://ujcontent.uj.ac.za/vital/access/manager/Index?site_name=Research%20Output (Accessed: Date).

The Effectiveness of Encryption Methods in Mitigating Information Technology Security Risks

by

TROY MOKOENA

(215043290)

A LIMITED SCOPE DISSERTATION

submitted in fulfilment of the requirements for the degree

MASTERS COMMERCII

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND FINANCIAL SCIENCES

at the

UNIVERSITY OF JOHANNESBURG

Supervisor: **Jacob Mamaile**

Co-Supervisor: **Rozanne Smith**

October 2016

ABSTRACT

Data protection is a critical area that is currently receiving much attention worldwide. Easy access to the internet and an increase in information transfer over communication networks contributes greatly to the need for data to be protected. Reports of data breaches from corporations and government institutions across the world have increased. Data breaches are mostly executed through the internet and other networks. Data loss and breaches can have significant consequences for concerned parties, such as reputational damage and litigation, when personal information is exposed to unauthorised persons. Mitigating controls, such as encryption methods, are generally implemented to protect data at rest and during transmission. Such controls, however, are useful only when they are effective in mitigating related risk exposure.

This study focuses on investigating whether the current encryption methods being used are perceived by IT security managers from the Big Four audit firms and Dimension Data, as effective in mitigating IT security risks. Although it has been reported in the literature that specific symmetric and asymmetric encryption methods are effective, this study revealed the following:

- Symmetric encryption is perceived in practice as a highly breakable method at 15%, least breakable at 75%, and rated as not yet used at 10%.
- Asymmetric encryption is perceived slightly higher, as a highly breakable method at 25%, least breakable at 62%, and not yet used at 13%.

UNIVERSITY OF JOHANNESBURG

Key words

Asymmetric; Ciphertext; Data protection; Encryption; Symmetric.

Acknowledgements

First and foremost, I would like to bless and thank the Almighty God for the enabling power and courage to start and complete this dissertation. Indeed, with Him all things are possible. I would also like to extend my gratitude to my lovely parents, loved ones and friends who have encouraged and supported me throughout the programme.

Last but not least, I would also like to appreciate my wonderful Supervisors, **Jacob Mamaile and Rozanne Smith**, for their technical guidance that was required to successfully complete this dissertation. Their efficiency and timely review made the programme very pleasant for me.

UNIVERSITY OF JOHANNESBURG

TABLE OF CONTENTS

ABSTRACT……... I

Acknowledgements…… II

List of Tables and Figures…… V

Acronyms and Abbreviations…….. VI

CHAPTER 1: STUDY INTRODUCTION

1.1 Introduction……... 1

1.2 Background and preliminary literature review…… 3

1.3 Problem statement…… 9

1.4 Research objectives……... 9

1.5 Research design and methods……... 9

1.5.1 Introduction…… 9

1.5.2 Philosophical paradigm…….. 10

1.5.3 Research choice…….. 10

1.5.4 Research strategy……... 10

1.5.5 Research limitations……... 11

1.6 Study contributions……... 12

1.7 Compliance with ethical standards……... 12

1.8 Chapter outline…….. 13

1.9 Conclusion…….... 13

CHAPTER 2: SYMMETRIC AND ASYMMETRIC ENCRYPTION

2.1 Introduction……... 14

2.2 Symmetric encryption…….. 16

2.2.1 Stream ciphers……... 18

2.2.1.1 RC4…… 18

2.2.2 Block ciphers…….. 19

2.2.2.1 Data encryption standard…… 19

2.2.2.2 Triple DES…….. 20

2.2.2.3 Advanced encryption standard…… 21

2.2.2.4 International data encryption algorithm…….. 22

2.2.2.5 Twofish……... 23

2.2.2.6 CAST…….. 24

UNIVERSITY OF JOHANNESBURG

2.2.2.7 RC6…… 24
2.2.2.8 Serpent…… 25
2.2.2.9 SEED…….... 26
2.2.2.10 Blowfish…… 27
2.3 Asymmetric encryption…… 28
2.3.1 RSA…… 30
2.3.2 Diffie-Hellman…….... 31
2.3.3 ElGamal…… 32
2.3.4 ECC…… 32
2.3.5 XTR…… 33
2.3.6 Digital signature algorithm…… 33
2.4 Conclusion…… 35
CHAPTER 3: RESEARCH METHODOLOGY
3.1 Introduction…….... 38
3.2 Population sample…… 38
3.3 Questions included in the research questionnaire…… 38
3.4 Validity of study results…… 39
3.5 Conclusion…… 39
CHAPTER 4: FINDINGS OF THE STUDY
4.1 Introduction…….... 40
4.2 Response rate…… 40
4.3 Participant demographics…….. 40
4.4 Research findings…….. 41
4.4.1 Symmetric encryption…… 41
4.4.2 Asymmetric encryption…….. 45
4.4.3 Encryption used by participants' organisations and clients……... 47
4.5 Conclusion…… 48
CHAPTER 5: STUDY CONCLUSIONS
5.1 Introduction…….... 49
5.2 Study overview…….. 49
5.3 Areas for future research……... 50
References…….. 51
Appendix A…… 63

UNIVERSITY OF JOHANNESBURG

List of Tables

Table 1: Consolidated 10-year performance on extensive use of encryption…… 7
Table 2: Drivers for encryption adoption……. 7
Table 3: Overview summary of symmetric and asymmetric encryption…… 35
Table 4: Participant demographics……... 41
Table 5: Triple DES encryption……... 42
Table 6: Twofish encryption…… 43
Table 7: Cast encryption…….. 44
Table 8: RC6 encryption…….. 44
Table 9: SEED encryption……... 45
Table 10: RSA encryption…… 46
Table 11: ECC encryption…… 47

List of Figures

Figure 1: Encryption process……... 4
Figure 2: Symmetric encryption…….. 5
Figure 3: Asymmetric encryption…… 5
Figure 4: Classes and types of symmetric encryption methods…… 15
Figure 5: Types of asymmetric encryption methods…… 16
Figure 6: Overall rating of symmetric encryption…… 42
Figure 7: Overall rating of asymmetric encryption…….. 46

UNIVERSITY OF JOHANNESBURG

Acronyms and Abbreviations

ADP	Armaments Development and Production
AES	Advanced Encryption Standard
ATM	Automated Teller Machines
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECT	Electronic Communications and Transactions
FIPS	Federal Information Processing Standards
GTAG	Global Technology Audit Guide
HTTPS	Hypertext Transfer Protocol
IBM	International Business Machines
IDEA	International Data Encryption Algorithm
IPES	Improved Proposed Encryption Standard
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
IT	Information Technology
KPMG	Klynveld Peat Marwick Goerdeler
NIST	National Institute of Standards Technology
PGP	Pretty Good Privacy
PWC	PricewaterhouseCooper
RICA	Regulation of Interception of Communications and Provision Communication-Related Information Act
TLS	Transport Layer Security
US	United States of America

UNIVERSITY OF JOHANNESBURG

CHAPTER 1
STUDY INTRODUCTION

1.1 Introduction

The information technology (hereafter, IT) environment is changing at a fast pace. Changes in IT result from constant developments in business and personal connectivity (Symantec, 2011:4). The rapid increase in platforms for social networking have resulted in an increase in the amount of information that people are sharing with each other in businesses and socially (Alassari, Muda & Ghazali, 2014:46).

These trends are being overshadowed by cloud computing, which makes files and applications available from any location through the internet (Huth & Cebula, 2011:1). Cloud computing means that corporate data is stored and accessed in multiple locations, which could result in security risks arising in the organisation (Huth & Cebula, 2011:1). It is therefore important that data be protected in these environments.

Hacking of computer systems is one of the common acts, where perpetrators obtain unauthorised access with the intention of stealing and modifying data, or for mere exploration. For instance, the dating site Ashley Madison, was hacked in 2015. A file containing personal information of the 32 million Ashley Madison users worldwide was made available to the public by the hackers (*Rand Daily Mail*, 2015). According to a study conducted by the Identity Theft Resource Centre, data breaches in 2014 in the United States of America increased by more than 25% from 2013 (Prince, 2014).

The results of the above studies indicate that attackers are becoming cleverer in discovering ways of obtaining unauthorised access to computer systems and resources. Research conducted in 2013 by Kaspersky Lab indicated that as a result of software vulnerabilities, more than a third of South African companies have reported incidences of data breaches (Alfreds, 2014). The research also indicated that 35% of the companies reported data security issues as a result of vulnerable software, while 11% of the companies reported critical data leaks due to software vulnerabilities (Alfreds, 2014).

UNIVERSITY OF JOHANNESBURG

Furthermore, in its July 2015 article, News24 Wire reported that the website of the South African Department of Arts was hacked (News24 Wire, 2015). It was indicated that the website was soon closed for investigation. The reasons for the hacking were, however, not reported (News24 Wire, 2015). This was the first reported hacking incidence of the South African government's website (s) since 2012. The *Mail and Guardian* reported in December 2012 that three South African websites were hacked by lone activists. The apparent reason for this hacking was due to South Africa's support for the Sahrawi Arab Democratic Republic in the Western Sahara (*Mail & Guardian*, 2012). These statistics further show a great need for the implementation of control measures to protect data and mitigate IT security risks.

IT security risks are managed by implementing various IT general and application controls. These include controls for the management of both logical and physical IT security risks (GTAG, 2012:10). The objective of implementing controls in the light of security risks is to achieve IT security, which assures confidentiality, integrity and availability of information systems and resources (Bhanot & Hans, 2015).

Confidentiality refers to the protection of data and information from unauthorised access (Bhanot & Hans, 2015:291). This is achieved by implementing access controls, encryption algorithms, network firewalls and antispyware software (GTAG, 2012:17). Integrity refers to the condition where information is maintained as accurate and consistent except when authorised changes are made (GTAG, 2013:6). Integrity is achieved by hashing, detective systems and digital signatures (Bhanot & Hans, 2015:291). Availability means ensuring that information and IT systems are available only to authorised persons as and when needed (Panmore Institute, 2015). This is achieved by fault-tolerant systems, redundancies and data backup controls (PWC, 2012:9). This study focuses only on encryption as opposed to the other methods of ensuring IT security.

Encryption is currently a popular and burning topic as a method of mitigating IT security risks and ensuring confidentiality. Encryption algorithms are regarded as one of the best methods for protecting data in this era of pervasive and constant technological changes (Ivey, 2013). Furthermore, encryption is considered as one of the best methods of protecting sensitive data, especially when the data is situated outside of the direct control of the organisation's IT department (Symantec, 2011:4). Due to these reasons, this study focuses only on encryption as

UNIVERSITY OF JOHANNESBURG

a method of data protection, as opposed to the previously mentioned methods of mitigating IT security risks.

Encryption is widely and frequently used as a method of data protection (Thawte, 2013). Encryption is a process of scrambling transmitted or stored information and making it unintelligible until it is unscrambled by the intended recipient (Ayushi, 2010:1). The use of encryption began during the Babylonian era, which can be traced back to 3000 B.C (Thawte, 2013). Encryption has been growing in importance due to the increasingly widespread use of the internet (Thawte, 2013).

Encryption methods have evolved from being used only in military and political settings to daily use by any user around the world (Malenkovich, 2013). A survey of the use of encryption by global enterprise was conducted in 2015 by the Ponemon Institute. It revealed an increased trend in the utilisation of encryption (Ponemon Institute, 2015:9) and indicated that the global enterprise use of encryption had increased by 16% from 2005 to 34% in 2014 (Ponemon Institute, 2015:9).

Reports for data breaches and leakages are increasing as reported above, and this correlates with the increase in enterprise use of encryption, therefore this study investigates the extent to which encryption methods are perceived in practice as effective in mitigating IT security risks.

UNIVERSITY OF JOHANNESBURG

The following section presents the background of IT security, a brief history of encryption and its role in IT security, some recent statistics of global encryption usage, and the role of IT audit in IT security.

1.2 Background and preliminary literature review

In today's world, computers and the data stored in them, is mostly secure when it is not connected to any network or the internet (Spitalnick, 2009:1). Therefore, it is vital to implement control measures such as encryption, in order to mitigate threats of data loss and breaches. The amount of critical and sensitive data stored in computer systems and transferred through the internet or other networks is growing at a fast pace, and this calls for effective mechanisms to protect data in these environments (Khan, Ismail & Zakuan, 2013:720).

Data security plays a critical role in that it ensures that data over computer systems (computer systems include networks and the internet) is protected. Data security over computer systems is achieved by implementing various control measures. Encryption is a common method that is implemented as a control measure in computer systems (Spivey & Echeverria, 2015:191). Data security over computer systems is ensured by applying different encryption methods (Jasim, Abbus, Harbaty & Salem, 2015). The application of encryption methods ensures data integrity, confidentiality and authentication. However, encryption methods are typically implemented as a measure against data loss and theft (O'Leary, Nelson, Green & Grahn, 2015).

In the encryption process, an encrypted message or data must be decrypted or deciphered using an encryption key before it can be read by the recipient. A readable message, called plaintext, is processed with a key through a mathematical algorithm, called a cipher, to change the message into unreadable ciphertext (O'Leary, Nelson, Green & Grahn, 2015). The ciphertext is then transmitted or sent to the recipient of a message. The recipient uses an encryption key to decode or change the ciphertext into readable plaintext (O'Leary, Nelson, Green & Grahn, 2015). Figure 1 below summarises the data encryption process.

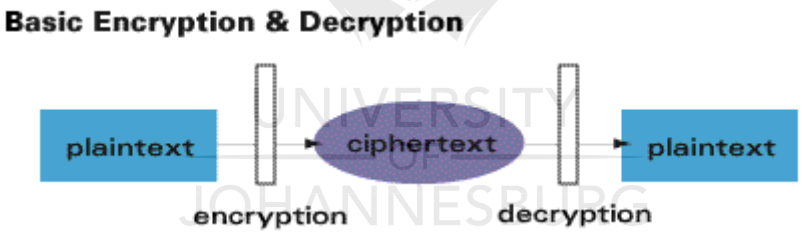

Figure 1: Data encryption process

Source: Simpson, 2015

The word encryption – crypt – comes from the Greek word *kryptos*, meaning hidden or secret (Seaman, 2012:2). Encryption technologies are applied to keep information secure from unintended audiences. Early encryption was developed in 1900 B.C. and involved converting or substituting messages with pictures, symbols and numbers to protect the content of messages when being transferred from one place to another (Raphael & Sundaram, 2010).

In the modern era, encryption is applied on computers using mathematical algorithms and secret keys to encrypt and decrypt data that cannot be executed by humans. Today's encryption is divided into two categories: symmetric and asymmetric algorithms (Santosh, 2010:6).

Symmetric algorithms use the same key (known as the secret key) to encrypt and decrypt a message (Ayushi, 2010:1).

In contrast to symmetric algorithms, asymmetric algorithms use one key (known as the public key) to encrypt a message, and a different key (known as the private key) to decrypt it (SANS Institute, 2003). In general, symmetric algorithms operate much faster than asymmetric algorithms.

In real applications, symmetric and asymmetric algorithms are often used together, with a public key algorithm encrypting a randomly generated encryption key, while the random key encrypts the actual message using a symmetric algorithm. This combination is commonly referred to as a digital envelope (Guo, Chen & Zhao, 2010:191). Symmetric and asymmetric algorithms are summarised in Figures 2 and 3.

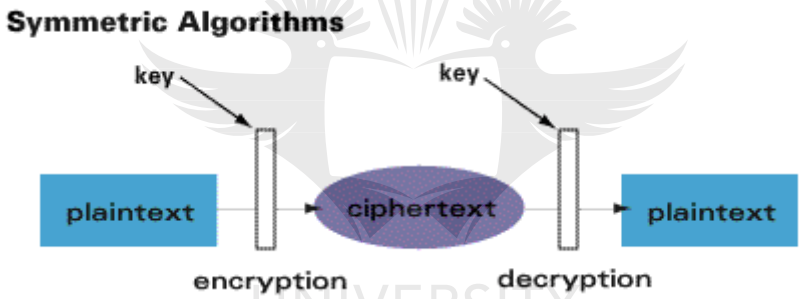

Figure 2: **Symmetric encryption using one key to encrypt and decrypt the message**

Source: Simpson, 2015

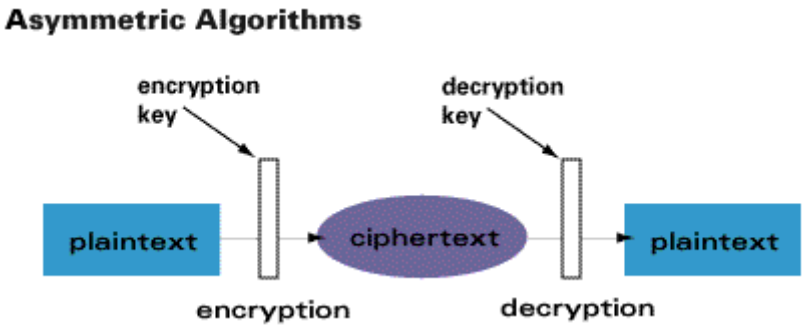

Figure 3: **Asymmetric encryption using different keys to encrypt and decrypt the message**

Source: Simpson, 2015

According to Edwards (2012), encryption methods are commonly used in the private sector because computers have increased in popularity in this sector. Computers in the private sector are used for commercial transaction processing, and this necessitates the need for adequate and effective security controls such as encryption (Petrovsky, 2015).

Encryption is one of the key control measures that is applied in ensuring security in transactional data (Edwards, 2012). There is a greater adoption of encryption within the private sector by certain industries such as financial services. Transactions are required to be very secure within financial services and therefore encryption is greatly applied (Petrovsky, 2015).

Encryption is deemed to be the best method in deterring data theft and hacking (Spitalnick, 2009:7). As a security tool, encryption is considered the best in ensuring data protection when data is stolen (Deshmukh & Qureshi, 2011:25). It is also regarded as the only best method for ensuring online security (Vijavan, 2013).

To effectively leverage on encryption, all critical business data and information should be encrypted at rest, with the emphasis placed on credit card information and other information deemed personal (Wood, 2011:36). Implementing encryption methods also supports an organisation in complying with certain laws and regulations for data protection. If the data is lost and the data was encrypted, a notification for such is not required (Wood, 2011:36).

UNIVERSITY OF JOHANNESBURG

A global encryption trends study conducted in 2015 by the Ponemon Institute revealed that encryption as a security solution adopted by organisations is growing. From 2005, there has been a significant reported increase in the number of organisations who are adopting an encryption strategy (Ponemon Institute, 2015:9). The Ponemon Institute started tracking the global enterprise-wide use of encryption in 2005 and has thus far prepared a consolidated 10-year performance on the extensive use and adoption of encryption methods. The trend is depicted in Table 1 below.

Table 1: **Consolidated 10-year performance on extensive use of encryption by enterprises**

Year (FY)	Percentage (%)
2005	16%
2006	20%
2007	19%
2008	22%
2009	23%
2010	23%
2011	25%
2012	27%
2013	30%
2014	34%

Source: Ponemon Institute, 2015:9

In 2011 the Ponemon Institute conducted a study on the drivers of encryption adoption. Table 2 below depicts the results.

Table 2: **Drivers for encryption adoption**

Driver	Percentage
To protect the company's brand or reputational damage resulting from a data breach.	45%
To lessen the impact of data breaches.	40%
To comply with privacy or data security regulations and requirements.	39%
To ensure that the organisation's commitments are honoured.	36%
To reduce the scope of compliance audits.	21%
To avoid having to notify customers or employees after a data breach occurs.	5%

Source: Ponemon Institute, 2012:8

In contrast to the positive results of encryption adoption indicated by the Ponemon Institute above, Anthes (2007:30) indicated that despite the growing trend in adoption of encryption technologies, there are enterprises that are still reluctant to implement and use encryption methods. Anthes (2007:30) indicated that performance implications were rated highest at 64% as the reason for not adopting encryption; the lowest reason was for the effort required to

modify applications, rated at 32%. Other factors mentioned by Anthes (2007:30) were: the cost of implementing encryption methods (60%); key management concerns (37%); and the implications that encryption methods have on disaster recovery (36%).

In South Africa, there is no legislation that governs the certification of encryption methods. Other than the certification of encryption, there are, however, several laws that govern its use. These laws are the Armaments Development and Production Act No. 57 of 1968 (hereafter, ADP), the Electronic Communications and Transactions Act No. 25 of 2002 (hereafter, ECT), and the Regulation of Interception of Communications and Provision of Communication-Related Information Act No.70 of 2002 (a monitoring Act also known as RICA).

The ADP Act regulates the use of encryption for military purposes. It states that a permit or license is required for all encryption software applied for military purposes (Michalson, 2012). However, a permit is not required for other uses of encryption. The ECT Act governs the registration of suppliers of encryption products. The Act requires that all suppliers register their particulars and products at the Department of Communications. Failure to register constitutes a criminal offence (Electronic Communications and Transactions Act, 2002).

Whereas, the Regulation of Interception of Communications and Provision Communication-Related Information Act (RICA) contains provisions that enable the security, law enforcement and intelligence agencies to fight crime and threats to national security (Michalson, 2012). The Act provides direction in obtaining the encryption key required to decrypt specific encrypted information (RICA, 2002).

IT audit plays a critical role in providing assurance on the adequate and effective implementation of security controls to prevent security risks. IT audit entails the auditing of an organisation's IT systems, operations, procedures and management processes (Suduc, Bizoi & Filip, 2010:45). Encryption is a control procedure that is implemented to mitigate security risks, and the IT audit role generally involves providing assurance that encryption procedures are adequately implemented and are functioning as intended. Furthermore, IT audit serves as a monitoring agent that reports on the continuous use of encryption and assesses whether the desired benefits are being realised from it.

UNIVERSITY OF JOHANNESBURG

1.3 Problem statement

IT security risk continues to grow as computers evolve and become more complex. The use of cloud computing and the vast amount of social networking creates opportunities for unauthorised access, which results in hacking activities, theft and loss of company data. In response to this, organisations implement control measures such as encryption, to mitigate possible IT security risks. However, although organisations are increasing their control measures to protect data from exploitation by hackers, breaches are still increasing at a fast pace. It is thus imperative that organisations implement controls that are effective and efficient in mitigating IT security risks (Hall & McGraw, 2014).

This study reports on the extent to which the various encryption methods are perceived as an effective means of protecting company data. In order to explore the stated research problem, the following main research question guided the study:

Are current encryption methods used perceived as being effective in mitigating IT security risks?

1.4 Research objectives

Main objective

- To establish whether current encryption methods are effective in mitigating IT security risks.

Sub-objectives

- To analyse and obtain an understanding of the functionality of available encryption methods;
- To evaluate the strengths of these encryption methods in protecting data; and
- To review and obtain an understanding of the shortfalls of the encryption methods.

1.5 Research design and methods

1.5.1 Introduction

This portion of the Chapter describes and discusses the research design and methods applied in answering the research problem stated in **1.3** above. The research design is distinguished and explained in three sections below, namely: philosophical paradigm, research choice, and research strategies. It concludes by explaining the research limitations.

UNIVERSITY OF JOHANNESBURG

1.5.2 Philosophical paradigm

This research is classified as an empirical study and follows a positivist approach. This approach is best suited to address the research problem stated in **1.3**, in the sense that authoritative knowledge and related experience is best suited to adequately address the stated research problem. Juma'h (2006:89), notes that a positivist approach emphasises that only those knowledge claims established directly from experience are truthful and verifiable. Therefore, in this study, the knowledge and experience of the IT security managers is used to address the stated research problem.

1.5.3 Research choice

A quantitative research methodology was followed in addressing the research question. This methodology was selected in light of the stated research question because it allows for data to be analysed and compared systematically, and for general conclusions to be made regarding the effective functioning of encryption methods. Questionnaires were used as a data collection instrument. Quantitative research methods involve collecting information which is analysed numerically. The results of such analyses are generally presented in tables and graphs using statistics (Siddiqui & Fitzgerald, 2014).

1.5.4 Research strategy

To facilitate and proceed with the quantitative approach selected, questionnaires were prepared to gather information from IT security experts (study participants) in pursuit of answering the stated research question. A questionnaire is a tool used to collect and record information regarding a particular issue of interest, and consists of a number of structured questions (Phellas, Bloch & Seale, 2011:184). Structured questions are closed-ended questions that are pre-selected by the researcher. There is generally low involvement of the researcher and a high number of respondents in structured questions (Zohrabi, 2013).

The structured questions sought to confirm the practical effective functioning of the studied encryption methods as well as the sourcing of encryption methods used by the participants. The questions were structured in a manner to facilitate information-gathering from the participants on their practical experiences and encounters regarding encryption methods.

The research questionnaire was circulated for completion by managers who are responsible for IT security in the Big Four auditing firms, and to Dimension Data, a global company

specialising in IT services, all based in the Johannesburg area within the Gauteng province. Firms situated in the Gauteng province, particularly in Johannesburg, were selected because more than 60% of the country's research and development, including IT, takes place in this province (South African Government, 2016). Furthermore, 29% of the employed people are located within the Gauteng province, hence it is likely that most of the skilled working people in this field are based within the capital (Johannesburg) of the Gauteng province.

The Big Four audit firms and Dimension Data were sampled from the population of organisations that provide IT security services. The Big Four audit firms were purposefully selected because they have a large scope of knowledge and skills which would be useful in answering the research problem (Organisation for Economic Co-operation and Development, 2009:7).

According to *Accounting Age*, PWC, Deloitte, KPMG and Ernst & Young are the Big Four auditing firms that were rated the top four in 2015 (*Accounting Age,* 2016). Dimension Data is listed in the top five of the largest IT companies that provide cyber (IT) security. Purposive sampling also refers to selective sampling, which entails selecting a sample that is tied to the research objectives (Palys, 2008), and was thus suitable for this study.

A manager who is responsible for IT security from each of the selected firms was targeted as the study participant and was requested to complete a research questionnaire. Therefore, a total of five completed questionnaires from each of the five selected firms was anticipated to be collected. These were subsequently analysed and presented in tables and graphs using statistics (Siddiqui & Fitzgerald, 2014) to answer the research question.

1.5.5 Research limitations

Due to a lack of programming knowledge and expertise, this research addressed the research problem through questionnaires with selected IT security managers. No direct and independent tests of the adequate and effective functioning of encryption methods was conducted. The research solely relied on the participants' responses and feedback in addressing the research problem. Further, the study did not focus on specific vendor-produced encryption methods, as there are currently no laws in South Africa governing the certification of encryption. Also, the study did not focus on encryption methods produced in South Africa only, as there is currently no law (s) that controls and regulates this.

1.6 Study contributions

The study aimed to obtain and provide an understanding of whether encryption as a control measure is effective in protecting data from IT security risks. The results of this study are intended to provide users with the knowledge required for assessing and selecting encryption methods. It will also assist encryption software vendors in adjusting their current encryption offerings to address some of the common threats and attacks to which the IT environment is susceptible.

1.7 Compliance with ethical standards

This study took caution and consideration of ethical issues regarding the following:

- Plagiarism: other people's work was respected by acknowledging the names of authors wherever their work was cited.
- Complying with the code of conduct and standards of the Information Systems Audit and Control Association (ISACA). The following areas were adhered to regarding the code of conduct and standards:
  - ✓ Integrity;
  - ✓ Confidentiality;
  - ✓ Objectivity.
- To ensure the anonymity of respondents, two boxes were placed at the respondents' IT department where the respondents' manually completed questionnaires were dropped, and were then collected by the researcher.
- Participants' identities remain anonymous and are referred to as "company A" and "company B" etc. in this study.
- All the information collected through the questionnaires was treated with the necessary confidentiality and was adequately protected from access by unauthorised parties.
- Participation was voluntary.

The university's ethical policy when using questionnaire, which provides for the right to privacy, confidentiality and anonymity, the right to equality, justice, human dignity/life and protection against harm, the right to freedom of choice, expression and access to information, right to the community and science community and informed consent / letters of request was duly considered in this study.

UNIVERSITY OF JOHANNESBURG

1.8 Chapter outline

This study consists of five chapters, outlined as follows:

Chapter 1: Introduction

Chapter 1 presents the background and preliminary literature review on encryption as a method of data protection. It further outlines the research problem, research questions, research design and methods, contribution of the study and compliance with ethical standards.

Chapter 2: Literature review – symmetric and asymmetric encryption

Chapter 2 presents background on symmetric and asymmetric encryption. It further outlines in detail the current symmetric and asymmetric encryption methods, as well as their related strengths and weaknesses.

Chapter 3: Research methodology

Chapter 3 outlines the research approach and methodology that was followed in conducting this study. Further, the scientific methods, justification of philosophical paradigm and data collection processes and methods are outlined in this chapter.

Chapter 4: Results and analysis

Chapter 4 presents the results of the study, of whether encryption methods are effective in mitigating IT security risks.

UNIVERSITY OF JOHANNESBURG

Chapter 5: Conclusion

Chapter 5 presents a summary and is the conclusion of the empirical study detailed in Chapters 1, 2, 3 and 4. Areas for future research are also outlined in this chapter.

1.9 Conclusion

This chapter has provided an introduction to the study and discussed the background of encryption, IT security and the role of audit in IT security. It further outlined the problem statement; research objectives; research methodology to be followed; study limitations and contributions; ethical compliance; and concluded by outlining the chapter compositions. The following chapter presents and discusses the literature on symmetric and asymmetric encryption.

CHAPTER 2
SYMMETRIC AND ASYMMETRIC ENCRYPTION

2.1 Introduction

Encryption is an important and powerful method that is used to protect data in computer systems (Masram, Shahare & Abraham, 2014:43). The purpose of encryption is to protect data from unauthorised parties (Annapoorna, Shravya & Krithika, 2014:98). For instance, when a browser is being used to process banking transactions, various cryptographic algorithms, such as encryption are applied to protect data that is sent to the bank (Forlanda, 2015).

Encryption is a component of cryptography, which is the study or science of secret communication (Forlanda, 2015). The objectives of cryptography are to ensure confidentiality, data integrity, authentication, authorisation and non-repudiation (NIST, 2016:31).

Confidentiality, on the other hand, refers to a situation where information or data is not disclosed to unauthorised parties (Bhanot & Hans, 2015:291). Confidentiality is achieved by applying encryption methods that make information unintelligible to unauthorised parties (NIST, 2016:31). Data integrity refers to a situation where information has not been changed by unauthorised persons or in an unauthorised manner since it was created, stored or transmitted (Bhanot & Hans, 2015:291). To achieve this, cryptographic mechanisms such as digital signature (also used for encryption) and message authentication codes are used (NIST, 2016:31).

Authentication as an objective of cryptography refers to establishing the integrity and origin of information (Bhanot & Hans, 2015:292). This objective is achieved by digital signatures or message authentication codes (National Institute of Standards Technology (hereafter NIST), 2016:31). Non-repudiation is similar to authentication in that it refers to establishing the integrity and origin of information, but different in that the integrity and origin can be verified by a third party (NIST, 2016:32). Authorisation however, refers to granting a user or a system the permission to perform a security function or an activity (Bhanot & Hans, 2015:292).

Encryption is a method used to achieve computer security by making messages non-readable by encoding them (Ayushi, 2010:1). In this modern era, encryption is considered to stem from

computer science and mathematics, and is connected to computer security, engineering and information theory (Charbathia & Sharma, 2014:1832). Encryption is more common in technologically advanced societies where it is used as a security measure in applications such as electronic commerce, computer passwords and automated teller machines (ATMs) (Gunasundari & Elangovan, 2014:78).

The data or information that is to be protected is referred to as plaintext when in its original form (NIST, 2016:26). By applying an encryption algorithm, the plaintext is changed into ciphertext. Ciphertext can be changed back to plaintext by applying a decryption key (NIST, 2016:36).

There are two types of encryption methods used in computer security, symmetric key encryption and asymmetric key encryption (Charbathia & Sharma, 2014:1832). Below is the summary of classes and types of symmetric encryption that are discussed in this chapter:

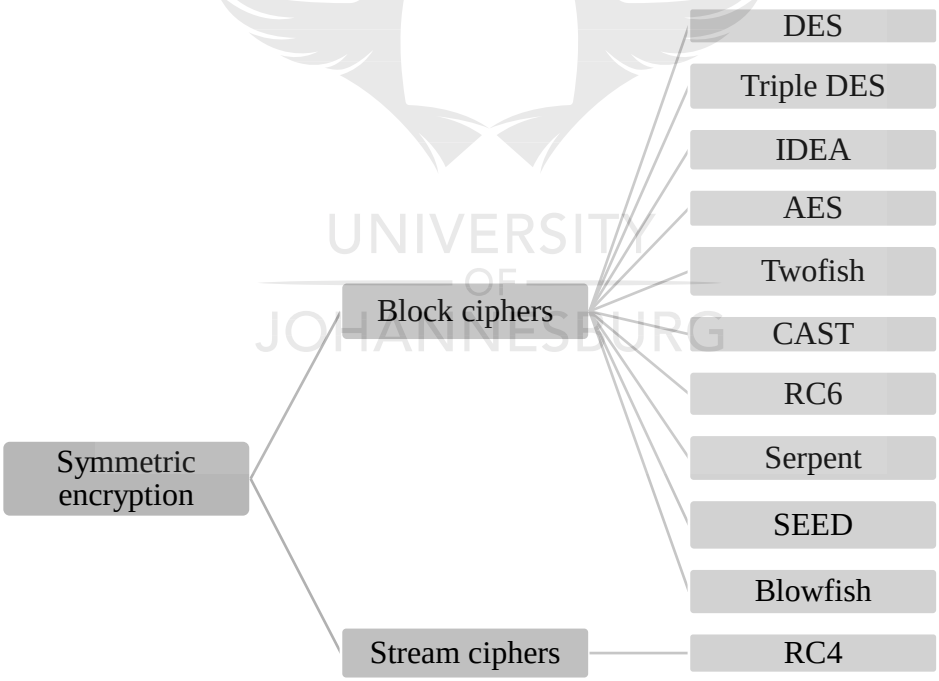

Figure 4: Classes and types of symmetric encryption methods

Source: Alam & Khan, 2013

While the following are the types of asymmetric encryption covered in this chapter:

UNIVERSITY OF JOHANNESBURG

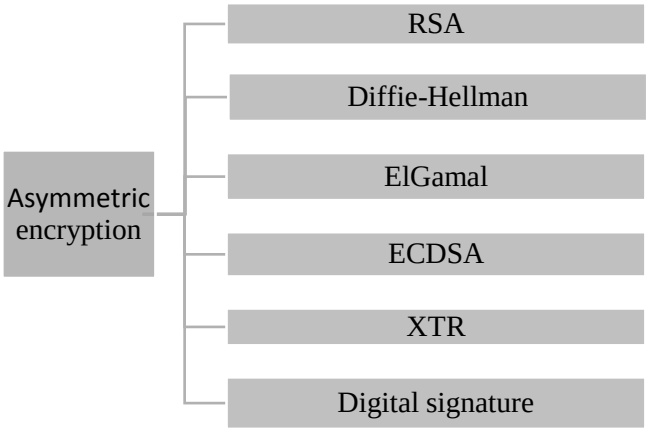

Figure 5: Types of asymmetric encryption methods

Source: Arya, Aswell & Kumar, 2015

2.2 Symmetric encryption

Symmetric key encryption (also called secret key encryption), is the common classic use of keys that uses one key to encrypt and decrypt data (iOS Developer Library, 2014). Symmetric key encryption is used to provide data confidentiality, authentication and integrity services as part of key establishment processes (NIST, 2016:36).

UNIVERSITY OF JOHANNESBURG

In symmetric encryption, prior to exchanging messages securely, both the sender and the receiver must agree on a key and its size (Ebrahim, Khan & Khalid, 2013:12). Key size means the size of a key file in bits; for example, 2048 bits is the key size for the RC4 cipher (Masram, Shahare, Abraham & Moona, 2014:43).

The symmetric encryption key is generally known by more parties, hence caution should be taken to ensure that the key is only disclosed to parties that are authorised to the data (NIST, 2016:35). The classic version of symmetric key encryption is the Caesar cipher, which is now easily broken (Christensen, 2010:1). Since the Caesar cipher, symmetric key encryption has been developed and strengthened from offering minimum security to nearly unbreakable security (iOS Developer Library, 2014).

Strong security, less time-consuming and high-speed performance are the main advantages of symmetric encryption (Pourali, Malakooti & Yektaie, 2014:440). Furthermore, symmetric methods are generally faster to execute on computers (Jasim, Abbas, Horbaty & Salem, 2015:83). Symmetric key encryption is classified as either being a stream cipher or a block cipher (Ayushi, 2010:1). Cipher refers to the process of changing a message into a secret (Pourali, Malakooti &Yektaie, 2014:440).

Stream cipher is an encryption method that encrypts a byte of plaintext at a time (Villanueva, 2015). Byte refers to a unit of a memory size (MyRepono, 2016). This cipher operates on a stream of bytes or bites, and is generally applied in securing data for wireless applications and terminals (Masram, Shahare, Abraham & Moona, 2014:44).

Furthermore, with the stream cipher, the encryption and decryption process embraces on a symbol by symbol at a time (Jasim, Abbas, Horbaty, Salem, 2015:83). Stream Ciphers can only remain secure if the key is never re-used and the generator for pseudorandom is unpredictable (Villanueva, 2015). RC4 is a type of stream cipher (Kadry & Smaili, 2010:85).

A block cipher, on the other hand, is a symmetric encryption method that encrypts and decrypts data on a fixed size of blocked data (Masram, Shahare, Abraham & Moona, 2014:44). Generally, block cipher sizes are 64, 128, 192 and 256 bits (Jasim, Abbas, Horbaty & Salem, 2015:83).

UNIVERSITY OF JOHANNESBURG

A large number of symmetric ciphers used today are block ciphers because of their strong security (Masram, Shahare, Abraham & Moona, 2014:44). Block ciphers are usually used in network applications when transmitting big files that require high security (Masram, Shahare, Abraham & Moona, 2014:44).

Furthermore, cryptanalysis for block ciphers is difficult as compared to stream ciphers (Jasim, Abbas, Horbaty & Salem, 2015:86). Cryptanalysis is when a ciphertext is being deciphered without knowing the key (Gehlot, Biradar & Singh, 2013:37). The commonly used block ciphers are DES, Triple DES, IDEA, AES, Twofish, CAST, RC6, Serpent, SEED and Blowfish (Alam & Khan, 2013:714).

Recommendation:

This section broadly discussed what symmetric encryption entails and pointed out that symmetric encryption is known for high-speed performance and strong security. It was further noted that symmetric encryption is classified as either a stream or block cipher. It was noted that RC4 is classified as a stream cipher and that DES, Triple DES, AES, IDEA, Twofish, CAST, RC6, Serpent, SEED and Blowfish are classified as block ciphers. The following section discusses both stream and block ciphers in detail.

2.2.1 Stream ciphers

In the above section, it was indicated that RC4 is a stream cipher; therefore, the following section broadly discusses RC4.

2.2.1.1 RC4

RC4 is a stream cipher with variable key size of up to 2048 bits (Chawla, Sehgal & Nagpal, 2015:55). The acronym RC stands for "Ron's Code" (Kadry & Smaili, 2010:85). It was developed in 1987 by Ronald L. Rivest (Gunasundari & Elangovan, 2014:80). This cipher was never officially released by RSA Security (Chawla, Sehgal & Nagpal, 2015:55). It was initially known as a trade secret; however, in September 1994, it was made available to a number of sites on the internet (Gunasundari & Elangovan, 2014:81).

UNIVERSITY OF JOHANNESBURG

RC4 is a pseudo random number generator; hence it is vital that in order to for this cipher to assure security, the same RC4 key should never be used to encrypt two different data streams (Charbathia & Sharma, 2014:1834). RC4 can be used in the Secure Sockets layer standards only if the communication between the web browsers and servers has been defined (Chawla, Sehgal & Nagpal, 2015:55).

RC4 is easy to develop and implement on both hardware and software (Kadry & Smaili, 2010:85). Furthermore, this cipher is deemed to be very fast in performance and it runs quickly in software (Gunasundari & Elangovan, 2014:81). The security of RC4 was credible until it became vulnerable to BEAST attack (Charbathia & Sharma, 2014:1834).

BEAST makes use of the type of cryptographic attack known as a chosen-plaintext attack (Sarkar, 2013:2). The attacker starts the attack by guessing the plaintext that is associated with a known ciphertext (Sarkar, 2013:2). The attacker then checks if the guess is correct by

accessing the encryption oracle to confirm if the encryption of the plaintext agrees with the known ciphertext (Sarkar, 2013:2).

BEAST attack is also executed by using a large number of encryptions of secret data (Imperva, 2015). The attacker does this by downloading a JavaScript from his website and running it in the victim's browser. The attacker would then repeatedly send Hypertext Transfer Protocol (HTTPS) requests to the victim web server to execute the attack (Imperva, 2015).

Recommendation:

As stated in the literature, RC4 was once considered strong in terms of security. There is, however, one known attack called BEAST, that has broken the RC4 encryption key. For this reason, the effective functioning of the RC4 cipher was not tested in this study through the research questionnaire.

2.2.2 Block ciphers

This section broadly discusses available block ciphers, starting with Data Encryption Standard:

2.2.2.1 Data encryption standard

The Data Encryption Standard (hereafter, DES) was established in 1977 by the US Federal Encryption Standard (Patil & Bhusari, 2014:64). DES uses a 56-bit key for each 64-bit block of data (Jasim, Abbas, Horbaty & Salem, 2015:83). For a number of years, DES was secure because fewer organisations had the computer power to crack it (Dogan, Ors & Saldamli, 2012:263). That was only until in 1998, when a group of cryptographers cracked the DES encryption key in less than three days (Bhanot & Hans, 2015:294).

DES keys are now considered very unsecure and can be broken in less than 24 hours (Dogan, Ors & Saldamli, 2012:263). According to Srinivas, Shanbhag and D'Souza (2014), the DES algorithm is insecure as it can be exploited by many attacks. Because of how quick and easy it was to break DES keys, the NIST stopped certifying DES as an encryption method (Bhanot & Hans, 2015:294). DES was officially withdrawn from the market in May 2005 (Bhanot & Hans, 2015:294). In its place, NIST introduced Triple DES as an extension of DES (Ebrahim, Khan & Khalid, 2013:13).

UNIVERSITY OF JOHANNESBURG

Recommendation:

The literature indicated that DES was discontinued as an encryption method due to its security weakness, hence its effective functioning in practice was not tested in this study through the research questionnaire.

2.2.2.2 Triple DES

Triple DES is an extension of the initial DES in that for security strength, it allows the same piece of data to run three times through the DES algorithm (Paul & Mandal, 2013:6). Triple DES affords a basic method of increasing DES key sizes to protect against attacks that were prone to the initial DES without having to design a new cipher algorithm (Alam & Khan, 2013:715).

Not only was Triple DES identified by NIST as an official replacement of DES, but it was also proposed by International Business Machines (IBM) in 1978 (Bhanot & Hans, 2015:294). Triple DES has a cumulative key size of between 112 to 168 bits, which is stronger than DES (NIST, 2016:37).

Furthermore, it is said that Triple DES is strong enough to defeat brute force attack, which was previously not attainable with the DES algorithm (Bhanot & Hans, 2015:295). The drawback of Triple DES is that it is slower in software computation compared to other new block ciphers (Paul & Mandal, 2013:7).

UNIVERSITY OF JOHANNESBURG

Although this cipher is deemed to provide adequate and strong security, it consumes a lot of time when compared to the initial DES (Bhanot & Hans, 2015:294). Furthermore, Triple DES was determined by cryptographers to be an undesirable long-term security solution (Ebrahim, Khan & Khalid, 2013:13).

Triple DES is, however, still deemed adequate by NIST (NIST, 2016:36). Triple DES is also still approved for use on US government systems, though it has been replaced by the AES sub-sections on most applications (Ebrahim, Khan & Khalid, 2013:13).

Recommendation:

From the above literature, it is deduced that Triple DES with the keys of 112 to 168 bits has not been broken, hence its effectiveness in providing adequate security was tested in this study through the research questionnaire. Question included in the research questionnaire: can the Triple DES encryption algorithm of between 112 and 168 bit-key be broken in practice?

2.2.2.3 Advanced encryption standard

The Advanced Encryption Standard (hereafter, AES) was created by Belgian cryptographers, Joan Daemen and Vincent Rijmen, in the early 2000s (Wood, 2011). AES uses key sizes of 128, 192 and 256 bits and was approved by NIST in 2001 (NIST, 2016:37). All these three key sizes are deemed adequate to protect the applications for the US Government Federal (NIST, 2016:37). Not only is this cipher sufficient to protect the US government data, but AES is used throughout the world in software and hardware to protect sensitive data (Bhanot & Hans, 2015:296).

AES algorithms are being referred to as state of the art because of their ability to provide adequate protection for sensitive information (Dogan, Ors & Saldamli, 2012:263). Each encryption size of AES causes the algorithm to behave differently and increases the key sizes (Paul & Mandal, 2013:7). AES has been adequately and effectively tested for many security applications (Kumar & Karthikeyan, 2012:23).

UNIVERSITY OF JOHANNESBURG

Furthermore, AES is very convenient and provides for flexibility in its implementation (Dogan, Ors & Saldamli, 2012:263). AES can be implemented on various platforms; however, this cipher thrives in small devices (Kumar & Karthikeyan, 2012:22). Furthermore, AES is the best method suitable for micro-payment processes (Pourali, Malakooti &Yektaie, 2014:440). It is also the best cipher to use during data transfer (Kumar & Karthikeyan, 2012:23). The increase in key sizes for AES allows for a larger number of bits to scramble the data (Jasim, Abbas, Horbaty & Salem, 2015:83). The downside about this is that it intensifies and increases the complexity of the algorithm (Paul & Mandal, 2013:7).

AES 128-bit keys have 10 rounds of which seven rounds have been broken thus far. The 192-bit keys of this cipher have 12 rounds of which eight rounds have been broken, and the 256-bit keys have 14 rounds of which nine rounds have been broken (Ferguson, Kelsey, Lucks, et al.,

2002). Schneier (2009) discovered key-related attacks on the full AES algorithm. These key-related attacks are theoretical, however no practical attacks on full AES have been reported.

Recommendation:

Because the full AES have been theoretically broken, this algorithm was not tested in this study through the research questionnaire.

2.2.2.4 International data encryption algorithm

International Data Encryption Algorithm (hereafter, IDEA) is a symmetric encryption that uses a block cipher (Basu, 2011:116). It was originally known as Improved Proposed Encryption Standard (IPES), and was developed in 1991 (Patil & Bhusari, 2014:64). According to Basu (2011), this cipher was developed by Professor J Massey and Dr X Lair as a replacement of DES standard (namely, DES and Triple DES). Due to DES susceptibility to many attacks, IDEA was considered one of the best ciphers after the discontinuing DES (Bhanot & Hans, 2015:303).

The IDEA cipher uses 128 key size and 64 bits of block data (Patil & Bhusari, 2014:64). IDEA has since been innovated and improved to provide security for network applications that demands high throughput (Bhanot & Hans, 2015:303). IDEA algorithm is known for its security strength and no practical attacks have been reported (Basu, 2011:118).

UNIVERSITY OF JOHANNESBURG

This cipher has been greatly improved in its operations to include three different algebraic groups for security purposes (Patil & Bhusari, 2014:64). Furthermore, IDEA is known for its resistance to both differential and linear analysis (Ebrahim, Khan & Khalid, 2013:13). However, the drawback of IDEA is that weaknesses in smaller keys were discovered by researchers (Patil & Bhusari, 2014:64).

Though this cipher has been acknowledged for its security strength, IDEA is susceptible to meet-in-the-middle attack, which has broken the full 8.5 round of IDEA (Biham, Dunkelman, Keller & Shamir, 2015). Also, full 8.5 rounds of IDEA have been broken by using a narrow-bicliques attack, which is similar to the bicliques attack which broke AES (Dey, 2015:179).

Recommendation:

Because the full rounds of the IDEA algorithm can be broken, the effectiveness of this cipher in practice was not tested in this study through the research questionnaire.

2.2.2.5 Twofish

The Twofish cipher was published in 1998. It is a symmetric encryption that has 128 block sizes and is able to accommodate keys of up to 256 sizes (Bhanot & Hans, 2015:299). According to NIST, Twofish came about as one of the options to replace the DES standard (Gupta, Murthy, Babu & Shankar, 2012:15).

The Twofish algorithm was developed by Bruce Schneier, Chris Hall, John Kelsey, Neils Ferguson, Doug Whiting and David Wagner (Ebrahim, Khan & Khalid, 2013:14). Twofish has been placed in the public domain for free use by anyone, and there is no patent attached to it (Bhanot & Hans, 2015:299).

Furthermore, Twofish applies the g-function, which doubles its cipher structure appearance and hence causes significant redundancy (Gehlot, Biradar & Singh, 2013:38). This cipher is also known for its lack of standardisation (Ebrahim, Khan & Khalid, 2013:14).

UNIVERSITY OF JOHANNESBURG

This cipher is efficient for software running in smaller processors, such as smart cards (Bhanot & Hans, 2015:299). It provides for encryption speed, balanced performance, set-up time and code size customisation (Gehlot, Biradar & Singh, 2013:37). Twofish provides adequate security but is slower in speed compared to the Blowfish cipher (Bhanot & Hans, 2015:301). This encryption algorithm is robust and resistive to related key, differential and slide attacks (Ebrahim, Khan & Khalid, 2013:16). Furthermore, no weak keys can be used to launch any related-key attack.

According to DiskSave (2016), Counterpane Systems invested one thousand hours in cryptanalising Twofish, and no attacks that break this cipher were identified. An encryption guru, Bruce Schneier, strongly recommends this algorithm for use as a data protection measure (Schneier, 2009). Furthermore, designers claimed an impossible differential attack on 6-round of Twofish as the best known attack on variants of this cipher (Moriai & Yin, n.d)

Recommendation:

According to the literature, no incidences of breaching the Twofish cipher have been identified. For this reason, the operating effectiveness of Twofish as a security measure is tested in this study through the research questionnaire. Question included in the research questionnaire: can the Twofish encryption algorithm of 256 bit-key be broken in practice?

2.2.2.6 CAST

The names of Carlisle Adams and Stafford Tavares, were abbreviated to CAST after they invented and developed CAST in 1996 (Ebrahim, Khan & Khalid, 2013:13) It is classified under encryption algorithms called Feistel ciphers (Krishnamurthy & Ramaswamy, 2009:28). As one of the classes of Feistel structure CAST uses eight fixed S-boxes (Ebrahim, Khan & Khalid, 2013:13).

This cipher uses 64 block sizes and supports between 40 and 128 bits of key lengths (Alam & Khan, 2013:715). CAST is differential and linear resistant, and there are no known ways of breaking this cipher (Krishnamurthy & Ramaswamy, 2009:28). CAST has been approved by the Canadian government for use by the Canadian Communications Security Establishment (Ebrahim, Khan & Khalid, 2013:13).

UNIVERSITY OF JOHANNESBURG

Recommendation:

No weaknesses of the CAST cipher have been indicated in the literature, hence the practical effectiveness of this cipher was confirmed through the research questionnaire. The literature stated that this cipher is supported by 40 to 128 bit keys. Question included in the research questionnaire: can the CAST encryption algorithm of 128 bit-key be broken in practice?

2.2.2.7 RC6

The RC6 symmetric encryption key block cipher is based on the RC5 algorithm, its predecessor which was discontinued due to its susceptible to attacks (Ebrahim, Khan & Khalid, 2013:14). It was developed in 1998 by Ron Rivest, Ray Sidney, Matt Robshaw and Yigun Lisa Yin (Charbathia & Sharma, 2014:1835). This cipher uses block sizes of 128 bits and can support 128, 192 and 256 bits' key sizes (Gupta, Murthy, Babu & Shankar, 2012:14).

RC6 was initially developed to meet the requirements of AES competition and was ultimately selected from its competitors to become the new US Federal Government AES encryption (Ebrahim, Khan & Khalid, 2013:14). RC6 provides for best security performance and compatibility in implementation (Charbathia & Sharma, 2014:1835).

This cipher is owned and patented by RSA Security (Ebrahim, Khan & Khalid, 2013:14), and is best known for its ability to consume less energy because it does not use look up tables (Gupta, Murthy, Babu & Shankar, 2012:14). Furthermore, RC6 offers great flexibility in number rounds and block sizes, therefore many corporations prefer it (Gunasundari & Elangovan, 2014:81).

RC6 provides for better security than that achieved in RC5, and also provides security for other various security attacks (Chaarbathia & Sharma, 2014:1835). This algorithm is resistant against most effective attacks on block ciphers such as differential and linear cryptanalytic attacks (Contini, Rivest, Robshaw & Yin, 1998).

Recommendation:

No security attacks on the RC6 cipher have been reported thus far; therefore, the effectiveness of this cipher in practice was tested through the research questionnaire. Question included in the research questionnaire: can the RC6 encryption algorithm of 128, 192 and 256 bit-key be broken in practice?

UNIVERSITY OF JOHANNESBURG

2.2.2.8 Serpent

Serpent block cipher was developed in 1998 by Ross Anderson, Lars Knudsen and Eli Biham (Ebrahim, Khan & Khalid, 2013:14). It has a block size of 128 bits and supports 128, 192 and 256 bits of key sizes (Sugier, 2011:2). Serpent was initially developed to meet the AES competition and was among the finalists; however, it lost to RC6 and achieved second place (Ebrahim, Khan & Khalid, 2013:14). Serpent is deemed a very fast and secure block cipher (Gupta, Murthy, Babu & Shankar, 2012:15). Furthermore, Serpent is widely acclaimed for its efficiency and excellent cryptographic strength (Sugier, 2011:1).

This cipher provides for easy and efficient implementation on hardware (Gupta, Murthy, Babu & Shankar, 2012:15). Due to look-up of tables, Serpent uses a lot of memory in its implementation (Sugier, 2011:2). This cipher has the ability to work with different

combinations of key lengths, hence it provides for adequate security (Gupta, Murthy, Babu & Shankar, 2012:15).

Serpent offers more conventional security compared to other ciphers offered by RSA security (Ebrahim, Khan & Khalid, 2013:14). This cipher is, however, not yet patented (Gupta, Murthy, Babu & Shankar, 2012:15). Another drawback of Serpent is that its key expansion is significantly slower (Sugier, 2011:2).

The security of Serpent is still widely acclaimed, as so far the best known attack has been only on 11 rounds of the 32 rounds of this algorithm (Dunkelman, Indesteege & Keller, n.d:1). The known attack is called a differential-linear attack (Kohno, Kelsey & Schneier, n.d:4).

Recommendation:

Although the security of Serpent is widely acknowledged, its effectiveness in practice was not tested in this study through the research questionnaire, as 11 rounds of this algorithm have been broken.

2.2.2.9 SEED

SEED is a block cipher that was developed in 1998 by the Korea Information Security Agency (Lu, Yap, Henricksen & Heng, 2014:117). SEED has a block and key size of 128 bits (Lu, Yap, Henricksen & Heng, 2014:117). This cipher is one of the classes of the Feistel Network structure (Pophale, Patil, Shelake & Sapkal, 2015:106). SEED is resistant to linear and differential attacks as well as to related key attacks (Sangpil, Deokho & Jaeyoung, 2012:161). In 2005 this cipher was adopted as an International Organisation for Standardisation (ISO) international standard (NIST, 2016).

This cipher is being used to provide security in e-commerce applications in the financial services in Korea (Lu, Yap, Henricksen & Heng, 2014:117). SEED was proposed by the Internet Engineering Task Force (IETF) and is included on PKCS #11 on Cryptographic Token Interface Standard (Lu, Yap, Henricksen & Heng, 2014:117).

This cipher provides simplicity of data backup and recovery process (Pophale, Patil, Shelake & Sapkal, 2015:106). A drawback of SEED is that the Feistel structure used by this cipher prevents it for parallel implementations (Sangpil, Deokho & Jaeyoung, 2012:164).

UNIVERSITY OF JOHANNESBURG

Recommendation:

No security attacks on the SEED cipher have been reported so far; therefore, the effectiveness of this cipher in practice was tested through the research questionnaire. Question included in the research questionnaire: can the SEED encryption algorithm of 128 bit-key be broken in practice?

2.2.2.10 Blowfish

The Blowfish cipher was developed in 1993 by Bruce Schneier (Bhanot & Hans, 2015:298). This cipher has a 64 block size and can support key sizes from 32 to 448 bits (Srinivas, Shanbhag & D'Souza, 2014:79). Blowfish operates in two parts: an encryption part and a key expansion part (Kumar & Karthikeyan, 2012:22). Blowfish is a class of Feistel cipher; it uses fixed S-boxes and is resistant to attacks such as differential and linear cryptanalysis (Alam & Khan, 2013:715). This, however, means that this cipher is not a feasible choice in limited memory space environments (Bhanot & Hans, 2015:298).

This cipher has been critically analysed and is considered as a strong encryption algorithm (Srinivas, Shanbhag & D'Souza, 2014:79). Blowfish offers the best security and encryption speed, providing an excellent encryption rate in software (Bhanot & Hans, 2015:299). Blowfish is unpatented and is available in the public domain for use by anyone (Ebrahim, Khan & Khalid, 2013:13).

UNIVERSITY OF JOHANNESBURG

Blowfish is fast and provides for simple implementation and adequate security (Ebrahim, Khan & Khalid, 2013:13). Furthermore, Blowfish contains the added functionality of key expansion, which makes this cipher difficult to crack (Srinivas, Shanbhag & D'Souza, 2014:79). Lastly, this cipher is considered better in processing time and throughput compared to DEA, Triple DES and AES (Kumar & Karthikeyan, 2012:22).

According to Bhanot and Hans (2015), no successful attacks against Blowfish have been reported thus far. For this reason, Blowfish is considered to be an excellent candidate to be deemed as a standard encryption algorithm (Kumar, Saini & Kumar, 2014:27). Despite its security strength, Blowfish is susceptible to weak key problems. However, no attack is known to have taken place against it (Kumar, Saini & Kumar, 2014).

Although, Blowfish is acclaimed for its security, its inventor, Bruce Schneier, is sceptical about this algorithm. In his 2007 security article, Schneier stated that he was surprised that people were still using the Blowfish algorithm, as he had thought that it would not survive a year of cryptanalysis (Schneier, 2009). Furthermore, Schneier concluded his article on security by recommending the Twofish cipher for use as a security measure as opposed to Blowfish.

The literature presents conflicting views regarding the Blowfish cipher. Some of the notable writers in the IT security field are of the view that this cipher is strong, and that it provides the best and adequate security.

Recommendation:

Because the inventor of the Blowfish cipher does not recommend it for use as a security measure, its effective functioning in practice was not tested in this study through the research questionnaire.

2.3 Asymmetric encryption

The second type of encryption method is called asymmetric encryption, also known as the public key algorithm (Arya, Aswell & Kumar, 2015:17). Asymmetric encryption uses different keys for encryption and decryption. This means that the decryption key is not derived from the encryption key; the two are practically different (Barukab, Khan, Shaik & Murthy, 2012:39). The encryption and decryption keys are, however, linked mathematically because both keys encrypt and decrypt the same message (Garg & Yadav, 2014:14). In asymmetric encryption, the encryption key, which is generally referred to as the public key, is known to everyone (Kak, 2016:6).

On the other hand, the decryption key (known as the private key), is kept a secret and is exclusively known by the recipient of the message (Arya, Aswell & Kumar, 2015:17). The security functionality of asymmetric encryption is that the knowledge of the encryption key (public key), does not automatically mean that the decryption key (private key) is also known.

Asymmetric encryption is important in that it can be used to transmit and distribute encryption keys (Barukab, Khan, Shaik & Murthy, 2012:38). Anyone can encrypt the message using the public key, however, only those who are in possession of the private key can decrypt the message (Annapoorna, Shravya & Krithika, 2014:98).

UNIVERSITY OF JOHANNESBURG

Asymmetric encryption solves the problem of exchanging encryption keys in a secure manner, which is not attainable in symmetric encryption. Furthermore, asymmetric encryption is efficient in that the data can be transferred securely even when parties did not have the opportunity to privately agree on the secret key (Barukab, Khan, Shaik & Murthy, 2012:39).

The public key conforms and adheres to the ISO and the American National Standards Institute (ANSI) (NIST, 2016:16). According to Garg and Yadav (2014), asymmetric encryptions are more secure compared to symmetric encryptions, and are best suited for internetworked systems installed in "untrusted" environments.

The security of asymmetric algorithms is enhanced because this algorithm undergoes a series of steps to check and verify the integrity of the data (Kak, 2016:6). Asymmetric algorithms are not only effective in hiding data, but can be used for non-repudiation and authentication (Qamar & Hassan, 2010:12).

The lack of assurance that the encryption key (public key) belongs to the expected party(s) is a major weakness of asymmetric encryption (Garg & Yadav, 2014:1191). The reason for this is that public keys are available to the public and perpetrators have an opportunity to create fraudulent keys and disguise them as genuine (Kak, 2016:5).

UNIVERSITY OF JOHANNESBURG

Asymmetric algorithms are inefficient operationally because they use long keys of over 1000 bits, and this makes sending and receiving long messages difficult (Qamar & Hassan, 2010:12). Due to this, asymmetric encryption is generally used for exchanging symmetric encryption keys and for digital signatures (Nateghizard, Bakhtiari & Maarof, 2014:2). To deal with asymmetric encryption key inefficiency challenges, hashing, which refers to the process of shortening characters, is generally used (Barukab, Khan, Shaik & Murthy, 2012:39).

According to Arya, Aswell & Kumar (2015) and Garg & Yadav (2014), RSA, Diffie-Hellman, ElGamal, ECDSA, XTR and Digital signature are the major types of asymmetric encryption, and these are discussed in detail in the sections below.

2.3.1 RSA

RSA, an abbreviation of Rivest, Shamir and Adleman, was invented in 1977 and is one of the most commonly used asymmetric algorithms (Annapoorna, Shravya & Krithika, 2014:98). RSA is one of the first asymmetric encryption to be used for both encryption and for digital signatures (for signing) (Arya, Aswell & Kumar, 2015:18).

RSA provides flexibility in its use, in that it can be used for both encryption and for digital signatures (Qamar & Hassan, 2010:13). For RSA to provide adequate security, its keys should be at least 1024 bits. Keys for about 2048 are said to provide adequate security for decades (Garg & Yadav, 2014:20). RSA is said to be still secure and is generally used in e-commerce (Qamar & Hassan, 2010:13).

This algorithm is secure because of the factorisation problem which says that it is difficult to factor large numbers (Arya, Aswell & Kumar, 2015:18). However, this factorisation can result in increased computation capacity when RSA both decrypts data and generates signatures (Garg & Yadav, 2014:18).

RSA keys are large due to the application of the arithmetic modulo; this possesses overhead challenges for resource constraint systems (Annapoorna, Shravya & Krithika, 2014:100). Generally, modules in the modular exponentiation are reduced to speed up the RSA and its efficiency (Arya, Aswell & Kumar, 2015:18).

UNIVERSITY OF JOHANNESBURG

Factoring of public key is regarded as one potential attack against the RSA cipher (Ambedkar & Bedi, 2011:242). However, achieving factoring of public keys on RSA algorithm is almost impossible because of the difficulty in factoring large numbers, considering that RSA uses large keys. If this is achieved, all messages written with the public key can be decrypted (SANS Institute, 2003).

Recommendation:

The literature indicated that RSA is secure and has survived years of cryptanalysis. Because no attacks on RSA have been reported, the effective functioning of this cipher was tested in this study through the research questionnaire. Question included in the research questionnaire: can the RSA encryption algorithm of 1024 bit-key be broken in practice?

2.3.2 Diffie-Hellman

The Diffie-Hellman was invented by Whitfield Diffie and Martin Hellman in1976 by using discrete logarithms in a finite field (Arya, Aswell & Kumar, 2015:18). This became the first creation within the asymmetric encryption family (Mimosa, 2015). Diffie-Hellman is a widely used algorithm for key exchanging and distribution (Garg & Yadav, 2014:18). It provides a platform for two users without any prior secrets to exchange secret keys through an insecure medium (Arya, Aswell & Kumar, 2015:18).

Diffie-Hellman is considered secure only when an appropriate mathematical group is used (Garg & Yadav, 2014:18). This algorithm is not installed on hardware (Mimosa, 2015). The Diffie-Hellman algorithm is limited only to the exchanging keys, which can be effective as long as the difficulty of computing discrete logarithms is ensured (Arya, Aswell & Kumar, 2015:18).

UNIVERSITY OF JOHANNESBURG

This algorithm has weaknesses against Logjam attacks, which facilitate man-in-the-middle attacks (Adrian, Bhargavan, Durumeric & Gaudry, 2015:1). Schneier (2015) agrees that Logjam is an attack against the Diffie-Hellman key-exchange protocol that is used in Transport Layer Security (TLS) connections. The Logjam attack gives an opportunity to the man-in-the-middle attacker to downgrade vulnerable TLS connections (Schneier, 2015).

Recommendation:

Because the literature indicated that Diffie-Hellman is susceptible to Logjam attacks, its security effectiveness in practice was not tested in this study through the research questionnaire.

2.3.3 ElGamal

ElGamal is an asymmetric encryption key which is based on the Diffie-Hellman key agreement (Arya, Aswell & Kumar, 2015:19). This algorithm was developed in 1984 by Taher Elgamal (Garg & Yadav, 2014:19). Similar to DSA, this algorithm provides security of at least 1024 key sizes (Arya, Aswell & Kumar, 2015:21). Furthermore, this algorithm is the predecessor of digital signature, hence it provides for both encryption and signatures (Annapoorna, Shravya & Krithika, 2014:100).

This algorithm is currently used in the recent versions of Pretty Good Privacy (PGP), namely GNU Privacy Guard software (Arya, Aswell & Kumar, 2015:19). ElGamal is inefficient compared to other asymmetric algorithms and its need for randomness generally makes it an unpreferred encryption method (Garg & Yadav, 2014:19). ElGamal is secure on the basis of maintaining the difficulty of computing discrete logarithms in an infinite field (Arya, Aswell & Kumar, 2015:19).

The ElGamal algorithm is susceptible to and is not secure under selected ciphertext attacks (Allen, 2008). ElGamal is also susceptible to stronger attacks that give the attacker an access to decryption oracle and which also allows them to perform memory dump of the decryption oracle (Kim, Cheon, Joyce, Lim, Mambo, Won & Zheng, 2001:15).

UNIVERSITY OF JOHANNESBURG

Recommendation:

Because ElGamal is susceptible to ciphertext attacks, its effective functioning in practice was not tested in this study through the research questionnaire.

2.3.4 ECC

ECC is abbreviated for Elliptic Curve Cryptography, and was developed in 1985 by Neal Koblitz and Victor Miller (Qamar & Hassan, 2010:14). It provides security for key sizes between 160 and 512 bits (Arya, Aswell & Kumar, 2015:20). ECC is based on the algebraic structure of elliptic curves over infinite values (Garg & Yadav, 2014:1191). This algorithm has emerged as the most secure and preferred encryption method compared to other asymmetric encryption methods (Bhanot & Hans, 2015:297).

ECC has the highest strength per bit compared to other asymmetric cryptography (Qamar & Hassan, 2010:14). Its security is strong on the basis that it is not feasible to find a discrete

logarithm of a random elliptic curve element by knowing the base point that is present in public domain (Arya, Aswell & Kumar, 2015:20).

Furthermore, ECC provides equivalent strong security with smaller key sizes, which results in lower power, faster computation, bandwidth usage and memory (Qamar & Hassan, 2010:14). ECC is deemed to be very effective and useful for mobile devices (Garg & Yadav, 2014:1191). To date, only 112-bit key for the prime field case and 109-bit key for the binary case of the ECC scheme has been broken (Majumdar & Maiti, 2015)

Recommendation:

The current 160-512 bit-key of the ECC algorithm has not been broken, hence its effectiveness in practice was tested in this study. Question included in the research questionnaire: can the ECC encryption algorithm of between 160 and 512 bit-key be broken in practice?

2.3.5 XTR

XTR is an asymmetric encryption; it stands for ECSR, which is an abbreviated from Efficient and Compact Subgroup Trace Representation. XTR uses the Diffie-Hellman key agreement protocol (Arya, Aswell & Kumar, 2015:19). XTR security is only assured as long as there are difficulties in solving discrete logarithm-related problems in the multiplicative group of a finite field (Nanda & Awasthi, 2012:838).

UNIVERSITY OF JOHANNESBURG

XTR is known for speed and its ability to generate keys very fast and of smaller sizes than the RSA cipher (Zhou, 2015:4466). The security level of XTR in bits is currently unknown (Nanda & Awasthi, 2012:838).

Recommendation:

Because the security level of XTR encryption is unknown in bits, it was not included in the research questionnaire when testing for effective functioning of encryption methods.

2.3.6 Digital signature algorithm

The Digital Signature Algorithm (hereafter, DSA) was proposed by NIST in 1991 as their digital signing algorithm, and was adopted by the US Federal Information Processing Standards

(FIPS) in 1993 (Arya, Aswell & Kumar, 2015:18). This algorithm provides security for 1024, 2048 and 3072 key sizes (Garg & Yadav, 2014:18).

DSA is an official standard of the US Federal government (Arya, Aswell & Kumar, 2015:19). DSA provides for integrity, authentication and non-repudiation (NIST, 2016:38). The functionality and efficiency of DSA is similar to that of ElGamal, although its level of efficiency is below that of the RSA cipher (Garg & Yadav, 2014:18).

DSA is always encrypted by the private key and decrypted by the public key (Qamar & Hassan, 2010:14). The major drawback of DSA is its fixed subgroup size (generator element order), which limits its security to only 80 bits (Garg & Yadav, 2014:18). Though DSA is widely used and accepted, it is susceptible to hardware attacks (Arya, Aswell & Kumar, 2015:19). Liu (2006) agrees with this claim: he stated that DSA generally suffers from hardware fault attacks.

Recommendation:

The literature indicated that DSA is a commonly used algorithm for signing electronically, and that its security has been compromised by hardware attacks. Due to this reason, the security effectiveness of DSA was not tested through the research questionnaire.

UNIVERSITY OF JOHANNESBURG

Below is an overview summary of both the types of symmetric and asymmetric encryption methods discussed above.

Table 3: Overview summary of symmetric and asymmetric encryption

Encryption Type	Invention Date	Security Strength
Types of symmetric encryption methods		
RC4	1987	2048 bits
DES	1977	56 bits
Triple DES	1998	122, 168 bits
AES	2000	128,192,256 bits
IDEA	1991	128 bits
Twofish	1998	128, 256 bits
CAST	1996	40, 128 bits
RC6	1998	128, 192, 256 bits
Serpent	1998	128,192, 256 bits
SEED	1998	128 bits
Blowfish	1993	32, 448 bits
Types of asymmetric encryption methods		
RSA	1977	1024 bits
Diffie-Hellman	1976	Unknown
ElGamal	1984	1024 bits
ECC	1985	160, 512 bits
XTR	Unknown	Unknown
DSA	1991	1024, 2048, 3072 bits

UNIVERSITY OF JOHANNESBURG

2.4 Conclusion

This chapter discussed various types of encryptions. It was discovered that encryption is divided into two classes: symmetric and asymmetric encryption. It was noted that symmetric encryption is classified as either stream or block cipher that uses one key to encrypt and decrypt data. On the other hand, asymmetric encryption is known as public key encryption that uses two different keys for encrypting and decrypting data.

Furthermore, the classifications and types of symmetric and asymmetric encryption were discussed in detail in this chapter, mainly looking at their security strengths and some of their notable advantages and disadvantages. The following symmetric encryption methods were not tested in this study through the research questionnaire because the literature identified security weaknesses as stated below:

- RC4 – the security of this algorithm has been broken by BEAST attacks;
- DES – this algorithm was discontinued due to its security weakness;
- AES – seven of the 10 rounds of 128 bit-key, eight of the 12 rounds of 192 bit-key and nine of the 14 rounds of 256 bit-key of this algorithm have been broken;
- IDEA – the full 8.5 rounds of this algorithm have been broken;
- Serpent – 11 of the 32 rounds of this algorithm have been broken;
- Blowfish – there were reported attacks on weak keys and the inventor of this algorithm does not recommend it for use as a data protection measure.

The following symmetric encryption methods were tested in this study through the research questionnaire, because so far, no security attacks were identified in the literature.

- Triple DES;
- Twofish;
- CAST;
- RC6;
- SEED.

UNIVERSITY OF JOHANNESBURG

The following asymmetric encryption methods were not tested in this study because the literature indicated weaknesses and/or security was unknown:

- Diffie-Hellman – this algorithm has been broken by Logjam attacks;
- ElGamal – this algorithm is susceptible to ciphertext attacks;
- XTR – the security of this algorithm is unknown;
- Digital Signature Algorithm – this algorithm is susceptible to hardware attacks.

The following asymmetric encryptions were tested in this study through the research questionnaire because the literature did not indicate any security weaknesses:

- RSA;
- ECC.

Chapter 3 discusses the research methodology that was followed in investigating and solving the research problem stated in Chapter 1.

UNIVERSITY
OF
JOHANNESBURG

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Introduction

This chapter is the extension of the research methodology that was outlined in Chapter 1. The population sample, questions included in the research questionnaire and validity of the results are discussed in this chapter. This chapter will conclude by outlining a brief overview of what was discussed.

3.2 Population sample

The population of the study was the reputable and credible organisations that provide IT security services. Due to their rich knowledge and scope, the Big Four audit firms and Dimension Data were purposively sampled from the population of organisations that provide IT security services.

3.3 Questions included in the research questionnaire

The literature (see Chapter 2) revealed encryption methods which are considered effective in mitigating information technology security risks. Therefore, the following questions were included in the research questionnaire to confirm with the participants the effectiveness of encryption methods as stated in the literature:

- Question 1.1: To establish whether the Triple DES encryption algorithm of between 112 and 168 bit-key can be broken in practice.
- Question 1.2: To establish whether the Twofish encryption algorithm of 256 bit-key can be broken in practice.
- Question 1.3: To establish whether the CAST encryption algorithm of 128 bit-key can be broken in practice
- Question 1.4: To establish whether the RC6 encryption algorithm of 128, 192 and 256 bit-key can be broken in practice.
- Question 1.5: To establish whether the SEED encryption algorithm of 128 bit-key can be broken in practice
- Question 1.6: To establish whether the RSA encryption algorithm of 1024 bit-key can be broken in practice.

UNIVERSITY OF JOHANNESBURG

- Question 1.7: To establish whether the ECC encryption algorithm of between 160 and 512 bit-key can be broken in practice
- Question 1.8: To establish the Symmetric Encryption methods used in the participants' organisations.
- Question 1.9: To establish the Symmetric Encryption methods used by the participants' clients.
- Question 1.10: To establish the Asymmetric Encryption methods used in the participants' organisations.
- Question 1.11: To establish the Asymmetric Encryption methods used by the participants' clients.

3.4 Validity of study results

The validity of the study results was ensured by employing a quantitative research approach. This approach allowed for the use of structured questionnaires to facilitate the quantification of responses. The objectivity in the study was ensured and maintained through the structured data collection. Furthermore, an in-depth literature review was conducted (see Chapters 1 and 2). The literature review served as the basis for the development of the structured questions that were included the research questionnaire.

UNIVERSITY OF JOHANNESBURG

3.5 Conclusion

The chapter discussed the population aspects of the study. It provided the justification for sample selection. Questions included in the research questionnaire were also outlined. The chapter concluded by discussing the justification for the validity of the results. The following chapter presents the study findings.

CHAPTER 4
RESULTS OF THE STUDY

4.1 Introduction

This chapter presents the results of the study. The results are the findings discovered through the gathering and analysis of information obtained through the completed questionnaires that answered the question of whether encryption methods are effective in mitigating information technology risks. The chapter starts by briefly outlining the response rate, participant demographics, and the detailed findings regarding the effectiveness of encryption methods as discussed in Chapter 2. The chapter concludes by presenting a summary of the study findings.

4.2 Response rate

A response rate total of 80% was achieved from all the participants. A breakdown of this is as follows: 75% response was achieved for the Big Four audit firms, meaning that three of the four firms completed the research questionnaire. A 100% response rate was achieved from Dimension Data.

4.3 Participant demographics

As previously stated, IT security professionals (managers) were the participants for this study. The participants had an overall average of 8.8 years working experience in the field of IT security, and their responsibilities included, amongst others, the following:

- Information security policy development;
- Information security policies implementation;
- Information security incident management;
- Leading, developing, and maintaining security roadmaps;
- Network design;
- Implementing IT security programs and tools;
- IT security risk assessment; and
- IT security compliance checks.

Source: Extract from research questionnaire

UNIVERSITY OF JOHANNESBURG

Table 3 shows a summary of the participants' educational and professional qualifications, their professional member bodies and their amount of working experience. Please note that the participating firms are referred to as firm A and etc. for ethics considerations:

Table 4: Participant demographics

Firm	Educational Qualification	Professional Qualification	Professional Member Body	Length of Working Experience
A	Not indicated	ITIL, CISCO, CCIE, F5, SOCP	Not indicated	9 years
B	National Diploma in Information systems	CISA, CISM	ISACA	7 years
C	B.Sc. Honours Degree in Information Systems.	CISA, CRISC, SAP GRC	ISACA	8 years
D	B.Com Informatics	CISSP, C|CISO	ISC2, ISF	11 years

Source: Research questionnaire (own analysis)

4.4 Research findings

This section outlines the research findings. The findings were analysed based on questionnaires completed by the participants indicated in **4.2** above. The questions were grouped into two categories, namely symmetric and asymmetric encryptions. For each category, questions were asked regarding the effectiveness of specific encryption (algorithm) methods as outlined in Chapter 2. The results are presented below.

4.4.1 Symmetric encryption

The objective of the symmetric encryption question category was to ascertain the effectiveness of Triple DES, Twofish, CAST, RC6 and SEED encryption algorithms in practice or in a real-life situation. Figure 4 below shows an overview summary of how the participants rated symmetric encryption.

UNIVERSITY OF JOHANNESBURG

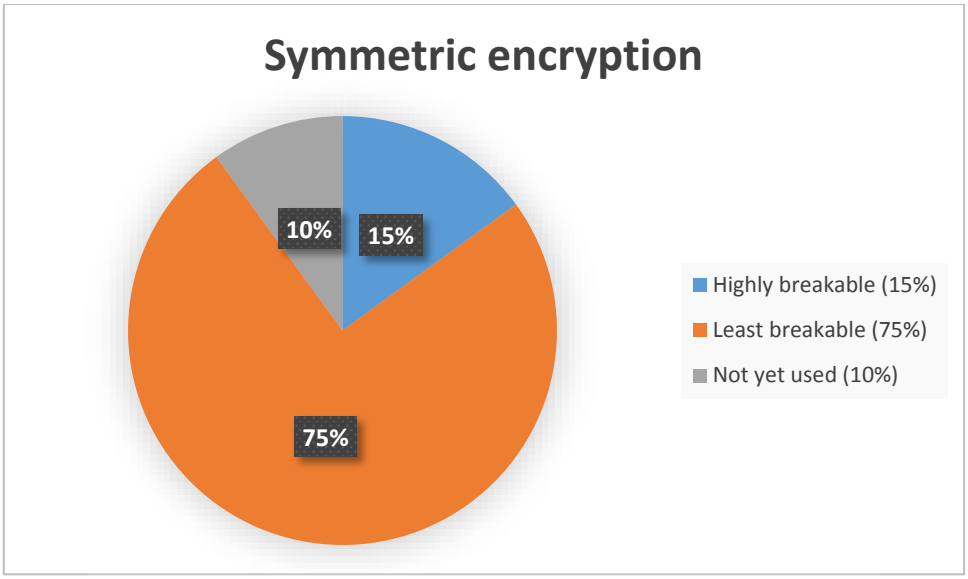

Figure 6: Overall rating of symmetric encryption

Source: Research questionnaire (own calculations)

Overall analysis: IT security managers perceived the symmetric encryption as least breakable at 75%, highly breakable at 15% and 10% was rated as not yet used.

Table 4 shows the detailed findings of each symmetric encryption method, presented in the following order: Triple DES, Twofish, CAST, RC6 and SEED.

Table 5: Triple DES Encryption

Please rate the effectiveness of the Triple DES encryption algorithm between 112 and 168 bit-key in practice	**Consolidated results (%)**	**Results from those who had used the encryption (%)**
Highly breakable	25	33,33333333
Least breakable	50	66,66666667
Not breakable	0	0
Not yet used	25	N/a
	100	**100**

Source: Questionnaire (own calculations)

UNIVERSITY OF JOHANNESBURG

Analysis and conclusion: of the IT security professionals who responded, 25% indicated that they had not used the Triple DES encryption in practice. Almost 67% of the 75% who had used the algorithm perceived as least breakable, while 33% indicated that this encryption is highly breakable.

Because no consensus was reached regarding the perception of Triple DES, no conclusion can be made regarding its effectiveness.

Table 6: Twofish Encryption

Please rate the effectiveness of the Twofish encryption algorithm of 256 bit-key in practice	**Consolidated results (%)**	**Results from those who had used the encryption (%)**
Highly breakable	0	0
Least breakable	100	100
Not breakable	0	0
Not yet used	0	N/a
	100	**100**

Source: Research questionnaire (own calculations)

UNIVERSITY OF JOHANNESBURG

Analysis and conclusion: all the participants indicated that they had used the Twofish encryption in practice, and all (100%) considered this algorithm to be least breakable.

Because a consensus was reached regarding the perception of Twofish encryption, it can therefore be concluded that it is effective.

Table 7: CAST Encryption

Please rate the effectiveness of the CAST encryption algorithm of 128 bit-key in practice	Consolidated results (%)	Results from those who had used the encryption (%)
Highly breakable	25	25
Least breakable	75	75
Not breakable	0	0
Not yet used	0	N/a
	100	**100**

Source: Research questionnaire (own calculations)

Analysis and conclusion: all the participants indicated that they had used the CAST encryption, as zero percent rated this algorithm as "not yet used". More than half (75%) considered this encryption as least breakable, whereas 25% considered the encryption as highly breakable.

Because no consensus was reached regarding the perception of CAST, no conclusion can be made regarding its effectiveness thereof.

UNIVERSITY OF JOHANNESBURG

Table 8: RC6 Encryption

Please rate the effectiveness of the RC6 encryption algorithm of 128, 192 and 256 bit-key in practice?	Consolidated results (%)	Results from those who had used the encryption (%)
Highly breakable	0	0
Least breakable	75	100
Not breakable	0	0
Not yet used	25	N/a
	100	**100**

Source: Research questionnaire (own calculations)

Analysis and conclusion: 25% of the respondents indicated that they had not used the RC6 encryption in practice. Of the remaining 75% who had experience with the algorithm, all (100%) considered it as least breakable.

Because a consensus was reached regarding the perception of Twofish encryption, it can therefore be concluded that it is effective.

Table 9: SEED Encryption

Please rate the effectiveness of the SEED encryption algorithm of 128 bit-key in practice	**Consolidated results (%)**	**Results from those who had used the encryption (%)**
Highly breakable	25	25
Least breakable	75	75
Not breakable	0	0
Not yet used	0	N/a
	100	**100**

Source: Research questionnaire (own calculations)

UNIVERSITY OF JOHANNESBURG

Analysis and conclusion: 75% of the respondents considered the SEED encryption as least breakable, while 25% considered it as highly breakable.

Because no consensus was reached regarding the perception of SEED, no conclusion can be made regarding its effectiveness thereof.

4.4.2 Asymmetric encryption

The objective of the asymmetric encryption question category was to ascertain the effectiveness of the RSA and ECC encryption algorithm in practice, or in real-life situations. Figure 5 presents an overview summary of how the participants rated asymmetric encryption.

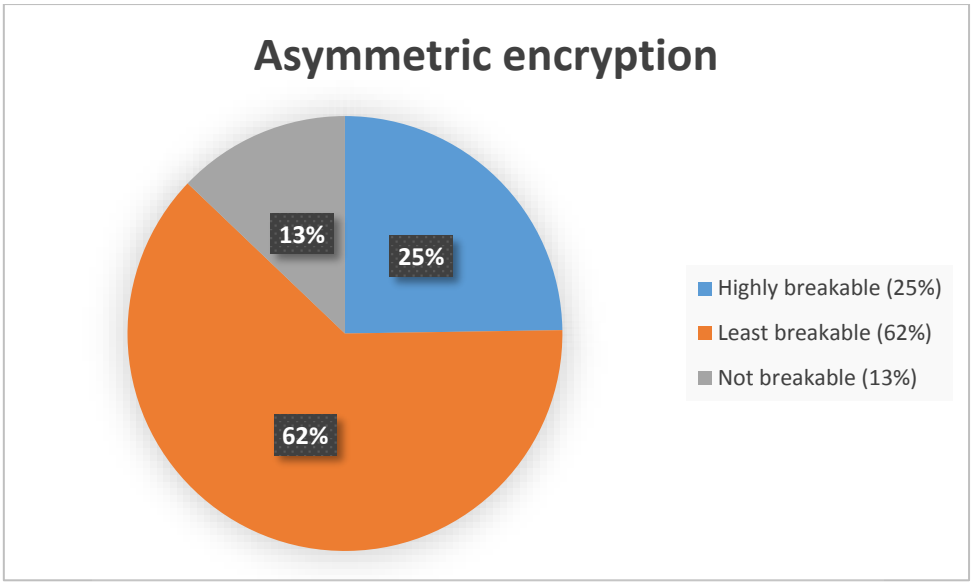

Figure 7: **Overall rating of asymmetric encryption**

Source: Research questionnaire (own calculations)

Overall analysis: the professionals highly rated the asymmetric encryption as least breakable at 62%. At 25%, asymmetric encryption was rated as highly breakable, which is high compared to the 15% rating on the same category for symmetric encryption. 13% of the participants indicated that they had not used some of the asymmetric encryptions. This percentage is slightly higher compared to the symmetric rating of 10%. Detailed findings of each asymmetric encryption method are presented in Tables 9 and 10, in the following order: RSA followed by ECC.

UNIVERSITY OF JOHANNESBURG

Table 10: RSA Encryption

Please rate the effectiveness of the RSA encryption algorithm of 1024 bit-key in practice	**Consolidated results (%)**	**Results from those who had used the encryption (%)**
Highly breakable	50	50
Least breakable	50	50
Not breakable	0	0
Not yet used	0	N/a
	100	**100**

Source: Research questionnaire (own calculations)

Analysis and conclusion: half of the respondents (50%) considered RSA as highly breakable, while the other half considered it as least breakable.

Because no consensus was reached regarding the perception of RSA, no conclusion can be made regarding its effectiveness thereof.

Table 11: ECC Encryption

Please rate the effectiveness of the ECC encryption algorithm of between 160 and 512 bit-key in practice	Consolidated results (%)	Results from those who had used the encryption (%)
Highly breakable	0	0
Least breakable	75	75
Not breakable	25	25
Not yet used	0	N/a
	100	**100**

Source: Research questionnaire (own calculations)

UNIVERSITY OF JOHANNESBURG

Analysis and conclusion: all the surveyed respondents had used the ECC encryption in practice and 75% of these considered this algorithm as least breakable, while 25% considered it as not breakable.

Because a consensus was reached regarding the perception of ECC encryption, it can therefore be concluded that it is effective.

4.4.3 Encryption used by participants' organisations and clients

The objective of the question category was to ascertain the symmetric and asymmetric encryption used by the participants' organisations and their clients. This category was completed by 50% of the participants who responded to the questionnaire. The following symmetric encryption methods were mentioned as being used by both the participants' organisations and by their clients:

- Skipjack, AES, RC5, Triple DES, Serpent, Twofish, Blowfish, TEA, XTEA, ARIA, CAST and RC4.

The following asymmetric encryption methods were mentioned as being used by the respondents in their organisations and by their clients:

- DSS, Elgamal, RSA, Yak, McEliece and Digital Signatures.

4.5 Conclusion

This chapter presented the results of how encryption methods are perceived by IT security managers as effective in mitigating IT security risks. The study revealed the following perceptions regarding the effectiveness of symmetric encryption methods:

- **Triple DES encryption**: no consensus on the perception regarding practical effectiveness of Triple DES.
- **Twofish encryption**: the encryption was perceived as effective in mitigating IT security risks.
- **CAST encryption**: no consensus on the perception regarding practical effectiveness of CAST.
- **RC6 encryption**: the encryption was perceived as effective in mitigating IT security risks.
- **SEED encryption**: no consensus the perception regarding practical effectiveness of SEED.

UNIVERSITY OF JOHANNESBURG

While the following perceptions were revealed regarding the effectiveness of asymmetric encryption:

- **RSA encryption**: no consensus on the perception regarding practical effectiveness of RSA.
- **ECC encryption**: the encryption was perceived as effective in mitigating IT security risks.

CHAPTER 5
STUDY CONCLUSIONS

5.1 Introduction

This chapter presents the overview, objectives results of the study. It concludes by outlining areas for future research.

5.2 Study overview

The study assessed how encryption methods are perceived by IT security managers, as effective in mitigating IT security risks. The literature revealed that incidences for data breaches are increasing at a faster pace. This then called for the investigation of whether data protection methods are effective in mitigating IT security risks, such as data breaches. Encryption as a method of data protection was selected for this study because it is regarded as the best method for protecting data in this era of pervasive technology.

Furthermore, it was noted in the literature that the global enterprise use of encryption is growing. This also motivated the study to focus on encryption methods. The literature revealed symmetric and asymmetric encryption methods which have not been broken by hackers. Questions regarding the perception of the practical effectiveness of those methods were prepared and asked to the IT security managers from the Big Four audit firms and Dimension Data.

UNIVERSITY OF JOHANNESBURG

Symmetric encryption was perceived as a highly breakable method at 15%, least breakable at 75%, not breakable at 0% and was rated as not used at 10%. Of the symmetric encryption methods, Twofish and RC6 were perceived as effective in mitigating IT security risks. Whereas, no consensus was reached regarding the perception on the effectiveness of Triple DES, CAST and SEED encryption methods.

Asymmetric encryption is perceived as a highly breakable method at 25%, least breakable at 62%, not breakable at 13% and none of the participants rated any of the asymmetric encryption as not yet used. ECC asymmetric encryption method was perceived as effective in mitigating IT security risks. While, no consensus was reached regarding the perception on the effectiveness of RSA method.

5.3 Areas for future research

The results of this study revealed that there is no consensus between literature and practice regarding the effectiveness of some of the encryption methods. The following issues are suggested subjects for future studies:

- Exploring how specific applications use Triple DES, CAST, SEED and RSA encryption algorithms, and how this relates to their operational effectiveness.
- Investigating the effectiveness of using Triple DES, CAST, Twofish, SEED, RC6, RSA and ECC encryption algorithms against prevalent and emerging security attacks.
- Assessing how encryption methods are perceived as effective by major IT service providers, such as Bytes Technology group.

UNIVERSITY OF JOHANNESBURG

References

Accounting Age. (2016). *The Top 50 Firms in 2015*. Available: http://www.accountancyage.com/static/top50-this-year (Accessed 21 July 2016).

Adrian, D., Bhargavan, K., Durumeric, Z. & Gaudry, P. (2015). *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*. Available: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf (Accessed 28 March 2016).

Alam, I., & Khan, MR. (2013). Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography. *International Journal of Advances Research in Computer Science and Software Engineering*, 3(10):713-720.

Alassari, AA., Muda, MB. & Ghazali, RB. (2014). Usage of Social Networking Sites and Technological Impact on the Interaction-Enabling Features. *International Journal of Humanities and Social Science*, 4(4):46.

Alfreds, D. (2014). *SA firms lose data in software breaches*. Available: http://www.kaspersky.co.za/ (Accessed 12 June 2015).

Ambedkar, BR. & Bedi, SS. (2011). A New Factorization Method to Factorize RSA Public Key Encryption. *IJCSI International Journal of Computer Science*, 8(6):242-247.

Annapoorna, S., Shravya, SK. & Krithika, K. (2014). A Review of Asymmetric Cryptography – RSA and ElGamal Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(5):98-105.

Anthes, G. (2007). Encryption: It's time. *Computerworld*, 41(21):27, 30.

Anonymous. (2002). How computer viruses work. *Plant Engineering*, 56(3); 80.

UNIVERSITY OF JOHANNESBURG

Arya, PK., Aswell, MS. & Kumar, V. (2015). Comparison Study of Asymmetric Key Cryptography Algorithm. *International Journal of Computer Science and Communication Networks*, 5(1):17-21.

Ayushi. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, 1(15):0975-8887.

Barukab, OM., Khan, AI., Shaik, MS. & Murthy, R. (2012). Secure Communication using Symmetric and Asymmetric Cryptographic Techniques. *International Journal of Information Engineering and Electronic Business*, 2:36-42.

Basu, S. (2011). International Data Encryption Algorithm – A Typical Illustration. *Journal of Global Research in Computer Science*, 2(7):116-118.

Bhanot, R. & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithm. *International Journal of Security and its Applications*, 9(4):289-306.

Biham, E., Dunkelman, O., Keller, N. & Shamir, A. (2015). New Attacks on IDEA with at Least 6 Rounds. *J Cryptol*, 28:209-239.

Charbathia, S. & Sharma, S. (2014). A Comparative Study of Rivest Cipher Algorithms. *International Journal of Information and Computation Technology*, 4(17):1831-1838.

Chawla, RV., Sehgal, R. & Nagpal, R. (2015). The RC7 Encryption Algorithm. *The International Journal of Security and its Applications*, 9(5):55-60.

Christensen, C. (2010). Caesar Ciphers. *HNR*, 304:1-19.

Contini, S., Rivest, RL., Robsham, B. & Yin, YL. (1998). *The Security of the RC6 Block Cipher*. Available: https://www.grc.com/r&d/rc6-security.pdf (Accessed 18 April 2016).

Deshmukh, AP. & Qureshi, R. (2011). Transparent Data Encryption – Solution for Security of Database Contents. *International Journal of Advanced Computer Science and Applications*, 2(3): 25-28.

UNIVERSITY OF JOHANNESBURG

Dey, PK. (2015). Analysis of the Security of AES, DES, 3DES and IDEA NXT Algorithm. *International Journal of Engineering Sciences and Research Technology*, 4(10):177-180.

DiskSave. (2016). *Encryption Methods Used – Twofish*. Available: http://www.disksave.com/twofish.htm (Accessed 15 September 2016).

Dogan, A., Ors, SB. & Saldamli, G. (2012). Analysis and comparing the AES architectures for their power consumption. *J IntellManuf*, 25:263-271.

Dunkelman, O. Indesteege, S. & Keller, N. (n.d). *A Differential-Linear Attack on 12-Round Serpent*. Available: http://www.ma.huji.ac.il/~nkeller/Crypt-conf8.pdf (Accessed 18 April 2016).

Ebrahim, M., Khan, S. & Khalid, UB. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer Applications*, 61(20):12-19.

Edwards, C. (2012). *Understanding the benefits and pitfalls of modern cryptography*. Available: http://www.newelectronics.co.uk/electronics-technology/understanding-the-benefits-and-pitfalls-of-modern-cryptography/39701/ (Accessed 20 January 2016).

Feigl, H. (2016). Positivism Philosophy. *Encyclopaedia Britannica*. Available: https://global.britannica.com/topic/positivism (Accessed 20 January 2016).

Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D. & Whiting, D. (2002). Improved Cryptanalysis of Rijndael. *Counterpane Internet Security, Inc.*, 213-230.

Forlanda, J. (2015). What *is the Difference between Encryption and Cryptography*? Available: http://www.brighthub.com/computing/enterprise-security/articles/65254.aspx (Accessed 10 March 2016).

Garg, N., & Yadav, P. (2014). Comparison of Asymmetric Algorithms in Cryptography. *International Journal of Computer Science and Mobile Computing*, 3(4):1190-1196.

UNIVERSITY OF JOHANNESBURG

Gehlot, P., Biradar, SR. & Singh, BP. (2013). Implementation of Modified Twofish Algorithm Using 128 and 192-bit keys on VHDL. *International Journal of Computer Applications*, 70(3):37-42.

Global Technology Audit Guide. (2010). *Information Technology Risks and Controls*. Available: http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag1%202nded.pdf (Accessed 14 September 2016).

Gunasundari, T. & Elangovan, K. (2014). A Comparative Survey on Symmetric Key Encryption Algorithms. *International Journal of Computer Science and Mobile Applications*, 2(2):78-83.

Gupta, VM., Murthy, KVS., Babu, Y. & Shankar, RS. (2012). Recent Performance Evaluation among AES Algorithm-MAS, RC6, RINJDAEL, SERPENT, TWOFISH. *International Journal of Science and Advanced Technology*, 2(2):11-19.

Guo, W., Chen, Y. & Zhao, X. (2010). A *Study on High-Strength Communication Scheme Based on Signed Digital Envelope*. Available: http://www.academypublisher.com/proc/isnns10/papers/isnns10p190.pdf (Accessed 20 January 2016).

Hall, JL. & McGraw, D. (2014). For Telehealth to Succeed, Privacy and Security Risks must be Identified and Addressed. *Health Affairs*, 33(2):216-221.

Huth, A. & Cebula, J. (2011). *The Basics of Cloud Computing. Available*: https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf (Accessed 26 January 2016).

Imperva. (2015). *Attacking SSL when using RC4; Breaking SSL with a 13-year-old RC4 weakness*. Available:http://www.imperva.com/docs/hii_attacking_ssl_when_using_rc4.pdf (Accessed 18 April 2016).

UNIVERSITY OF JOHANNESBURG

iOS Developer Library. (2014). *Cryptography Concepts in Depth.* Available: https://developer.apple.com/library/ios/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html (Accessed 10 March 2016).

Ivey, V. (2013). *Tips to Keep Your Data Secure in the Cloud*. Available: http://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html (Accessed 21 September 2015).

Jasim, O., Abbus, S., Harbaty, E. & Salem, AB. (2015). Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm. *Information Security*, 6(2):82-92.

Juma'h, A. (2006). Empirical and Realistic Approaches of Research. *Inter Metro Business Journal*, 2(1):88. Available: http://ceajournal.metro.inter.edu/spring06/jumah0201.pdf (Accessed 4 August 2015).

Kak, A. (2016). Lecture Notes on Computer and Network Security. Lecture 10: Key Distribution for Symmetric Key Cryptography and Generating Random Numbers. Available: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf (Accessed 29 March 2016).

Kadry, S. & Smaili, M. (2010). An Improvement of RC4 Cipher using Vigenere Cipher. *International Journal of Computational Intelligence and Information Security*, 1(3):83-92.

Khan, MN., Ismail, NZ. & Zakuan, N. (2013). Benefits of financial reporting in developing countries: Evidence from Malaysia. *African Journal of Business Management*, 7(9):719-726.

Kim, S., Cheon, JH., Joyce, M., Lim, S., Mambo, M., Won, D. & Zheng, Y. (2001). Strong Adaptive Chosen-Ciphertext Attacks with Memory Dump. *Cryptography and Coding*, 114-127.

Kohno, T., Kelsey, J. & Schneier, B. (n.d). Preliminary Cryptanalysis of Reduced-Round Serpent: Third AES Candidate Conference. *Counterpane Internet Security*, (3):195-211.

UNIVERSITY OF JOHANNESBURG

Krishnamurthy, GN. & Ramaswamy, V. (2009). Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images. *International Journal of Network Security & Its Applications*, 1(1):28-33.

Kumar, R. Saini, B. & Kumar, B. (2014). A Novel Approach to Blowfish Encryption Algorithm. *International Journal of Advance Foundation and Research in Science & Engineering*, 1(2):26-34.

Kumar, MA., & Karthikeyan, S. (2012). Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. *I.J. Computer Network and Information Security*, 2:22-28.

Wood, L. (2011). The Clock is Ticking for Encryption. *Computerworld*, 45(6):32, 34, 36.

Liu, S. (2006). *A CRT-RSA Algorithm Secure Against Hardware Fault Attacks*. Available: https://www.computer.org/csdl/proceedings/dasc/2006/2539/00/25390051.pdf (Accessed 18 April 2016).

Lu, J., Yap, W., Henricksen, M. & Heng, S. (2014.) Differential attack on nine rounds of the SEED block cipher. *Information processing letters*, 114:116-123.

Mail & Guardian. (2012). *Three SA government websites hacked*. Available: http://mg.co.za/article/2012-12-09-three-government-websites-hacked (Accessed 18 September 2015).

Majumdar, S. & Maiti, A. (2015). Advanced Security Algorithm Using QR Code Implemented for an Android Smartphone System. *International Journal of Advanced Research in Computer Science and Management Studies*, 3(5):21-31.

Malenkovinch, S. (2013). *Reasons to Encrypt Your Data*. Available: https://blog.kaspersky.com/encrypt-your-data/1889/ (Accessed 25 January 2016).

Masram, R., Shahare, V., Abraham, J. & Moona, R. (2014). Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based of Various File Features. *International Journal of Network Security & Applications*, 6(4):43-52.

UNIVERSITY OF JOHANNESBURG

Michalson, L. (2012). *Cryptography laws in South Africa*. Available: http://www.michalsons.co.za/cryptography-and-the-ect-act/3266 (Accessed 21 September 2015).

Mimosa, M. (2015). *Prime Diffie-Hellman weaknesses may be key to breaking crypto.* Available: https://threatpost.com/prime-diffie-hellman-weakness-may-be-key-to-breaking-crypto/115069/ (Accessed 29 March 2016).

Moriai, S. & Yin, YL. (N.d). *Cryptanalyzing Twofish*. Available: https://www.schneier.com/twofish-analysis-shiho.pdf (Accessed 18 April 2016).

MyRepono. (2016). *Understanding files sizes*. Available: http://myrepono.com/faq/4 (Accessed 07 April 2016).

Nanda, AK. & Awasthi, LK. (2012). XTR Cryptosystem for SMS Security. IACSIT. *International Journal of Engineering and Technology*, 4(6):826-839.

Nateghizard, M., Bakhtiari, M. & Maarof, MA. (2014). Secure Searchable Based Encryption in Cloud Computing. *International Journal of Advanced in Software Computing*, 6(1):2-13.

National Institute of Standards and Technology. (2016). Computer Security. *NIST Technical Series Publication*, 1(4):1-147.

News24 Wire. (2015). *SA government website taken down by hackers*. Available: http://mybroadband.co.za/news/security/132256-sa-government-website-taken-down-by-hackers.html (Accessed 18 September 2015).

O'Leary, D., Nelson, J., Green, P. & Grahn, A. (2015). *Key Elements of a Successful Encryption-Strategy*. Available: http://focus.forsythe.com/articles/364/7-Key-Elements-of-a-Successful-Encryption-Strategy (Accessed 20 January 2016).

Palys, T. (2008). Purposive Sampling. *The Sage Encyclopaedia of Qualitative Research Methods*, (6):697-698.

UNIVERSITY OF JOHANNESBURG

Panmore Institute. (2015). *The CIA Triad: Confidentiality, Integrity and Availability*. Available: http://panmore.com/the-cia-triad-confidentiality-integrity-availability (Accessed 17 February 2016).

Parylo, O. (2012). Qualitative, Quantitative or Mixed Methods: An analysis of research design in articles on principal professional development. *International Journal of Multiple Research Approaches*, 6(3):297-313.

Patil, S. & Bhusari, V. (2014). An Enhancement in International Data Encryption Algorithm for Increasing Security. *International Journal of Application or Innovation in Engineering and Management*, 3(8):64-70.

Paul, M. & Mandal, JK. (2013). A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept. *International Conference on Information Technology, Electronics and Communications*.

Petrovsky, C. (2015). *Best Practices: Encryption for Financial Services*. Available: http://www.centritechnology.com/encryption-best-practices-financial-services/ (Accessed 20 January 2016).

Phellas, CN. Bloch, A & Seale, C. (2011). *Structured Methods: Interviews, Questionnaires and Observation*. Available: http://www.sagepub.com/sites/default/files/upm-binaries/47370_Seale_Chapter_11.pdf (Accessed 22 January 2016).

Ponemon Institute. (2012). *2011 Global Encryption Trends Study*. Available: http://www.ponemon.org/local/upload/file/2011_Global_Encryption_Trends_Study_FINAL.pdf (Accessed 21 September 2015).

Ponemon Institute. (2015). *Global Encryption & Key Management Trends Study*. Available: http://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=5&ved=0CDMQFjAEahUKEwjL3viy2YfIAhVoOdsKHeIDAmE&url=http%3A%2F%2Favensus.nl%2Ffile%2Fdownloads%2F2015_Global_Encryption_Trends_Study.pdf&usg=AFQjCNH5Auo2_lfN-_RweaUsot74oUZvgA&bvm=bv.103073922,d.d24 (Accessed 21 September 2015).

UNIVERSITY OF JOHANNESBURG

Pophale, K., Patil, P., Shelake, R. & Sapkal, SW. (2015). Seed Block Algorithm: Remote Smart Data-Backup Technique for Cloud Computing. *International Journal of Advanced Research in Computer and Communications Engineering*, 1(3):105-107.

Pourali, A., Malakooti, M. & Yektaie, M. (2014). *A Secure SMS Model in E-Commerce Payment Using Combined AES and ECC Encryption Algorithms*. Proceedings at the International Conference on Computing Technology and Information Management. Available: http://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjPsZD9oeXLAhXIExoKHfIzA_sQFgggMAA&url=http%3A%2F%2Fsdiwc.net%2Fdigital-library%2Fweb-admin%2Fupload-pdf%2F00001064.pdf&usg=AFQjCNFGl2PPb2w3wjwUO4NyBW6SJLSe2g&bvm=bv.117868183,d.bGQ (Accessed 27 March 2016).

Prince, B. (2014). Data Breaches of 2014. *InShare*. Available: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html (Accessed 11 June 2015).

PricewaterhouseCoopers. (2012). *Fortifying your defences: The role of internal audit in assuring data security and privacy*. Available: https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-internal-audit-assuring-data-security-privacy.pdf (Accessed 27 March 2016).

Qamar, T. & Hassan, R. (2010). *Asymmetric-Key Cryptography for Contiki*. Master of Science Thesis in the Programme Networks and Distributed Systems. Available: http://publications.lib.chalmers.se/records/fulltext/129176.pdf (Accessed 26 March 2016).

Rand Daily Mail. (2015). *Ashley Madison hack: Cheating South Africans' affairs revealed by hackers*. Available: http://www.rdm.co.za/lifestyle/2015/08/20/ashley-madison-hack-cheating-south-africans-affairs-revealed-by-hackers (Accessed 18 September 2015).

Raphael, AJ. & Sundaram, V. (2010). Cryptography and Steganography – A Survey. *International Journal of Computer Applications*, 2(3):626-630.

UNIVERSITY OF JOHANNESBURG

Sangpil, L., Deokho, K. & Jaeyoung, Y. (2012). An Efficient Block Cipher Implementation on Many-Core Graphics Processing Units. *Journal of Information Processing Systems*, 8(1):159-174.

Santosh, KY. (2010). *Some Problems in Symmetric and Asymmetric Cryptography*. Available: http://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CCIQFjABahUKEwigvf_W1IfIAhUOINsKHdhEDAg&url=http%3A%2F%2Fwww.iacr.org%2Fphds%2F31_SantoshKumarYadav_SomeProblemsinSymmetricndAsymm.pdf&usg=AFQjCNEySp7Ehynqxto1Nv2-PlCKQhKxEA (Accessed 21 September 2015).

SANS Institute. (2003). *Cryptanalysis of RSA: A Survey*. Available: https://www.sans.org/reading-room/whitepapers/vpns/cryptanalysis-rsa-survey-1006 (Accessed 18 April 2016).

Sarkar, PG. (2013). *Attacks on SSL: A Comprehensive Study of BEAST, Crime, Time, Breach, Lucky 13 and RC4 Biases*. Available: http://www.cse.iitk.ac.in/users/cs300/2014/home/~karanb/cs300A/techpaper-review/5B.pdf (Accessed 18 April 2016).

Schneier, B. (2009). New Attacks on AES. Available: https://www.schneier.com/blog/archives/2009/07/new_attack_on_a.html (Accessed 16 April 2016).

Schneier. B. (2015). *The Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange*. Available: https://www.schneier.com/blog/archives/2015/05/the_logjam_and_.html (Accessed 16 April 2016).

Seaman, K. (2012). *Kryptos*. Available: https://repositories.tdl.org/ttu-ir/bitstream/handle/2346/45181/SEAMAN-THESIS.pdf?sequence=2 (Accessed 21 September 2015).

UNIVERSITY OF JOHANNESBURG

Siddiqui, N. & Fitzgerald, JA. (2014). Elaborated integration of qualitative and quantitative perspectives in mixed methods research: A profound enquiry into the nursing practice environment. *International Journal of Multiple Research Approaches*, 8(2): 137-147.

Simpson, S. (2015). *Cryptography*. Available: http://www.linkmix.in/cryptography/ (Accessed 22 January 2016).

Sourabh, B. & Bibhuti, BM. (2015). Evolution, Growth and Challenges in E-commerce Industry: A Case of India. *Sumedha Journal of Management*, 4(1).

South Africa. (2002). Communication-related Information Act. Act 70 of 2002. Available: http://www.internet.org.za/ricpci.html (Accessed 21 September 2015).

South Africa. (2002). Electronic Communication and Transactions Act 25 of 2002. Available: http://www.internet.org.za/ect_act.html (Accessed 21 September 2015).

South African Government. (2016). South African's Provinces. Available: http://www.gov.za/about-SA/south-africas-provinces (Accessed 29 November 2016).

Spitalnick, A. (2009). Understanding Encryption and Its Role in Security. *CPA Practice Management Forum*, 5(7):7-10.

Spivey, B. Echeverria, J. (2015). Protecting your Big Data Platform. *Hadoop Security*. Available: https://books.google.co.za/books?id=VXEJCgAAQBAJ&pg=PA191&lpg=PA191&dq=encryption+a+common+method+for+data+protection&source=bl&ots=e5ZXLt8Fts&sig=r0RXOjP6JEd1LkR9J6zsXi-G8Sc&hl=en&sa=X&ved=0ahUKEwjOw5ng_7fKAhVExRQKHRJFCs4Q6AEIMzAE#v=onepage&q=encryption%20a%20common%20method%20for%20data%20protection&f=false (Accessed 20 January 2016).

Srinivas, BL., Shanbhag, A. & D'Souza, AS. (2014). A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm. *International Journal of Innovative Research in Computer and Communications Engineering*, 2(5):77-88.

UNIVERSITY OF JOHANNESBURG

Suduc, AM., Bizoi, M. & Filip, FG. (2010). Audit for Information Systems Security. *Informatica Iconomica*, 14(1): 43-48.

Sugier, J. (2011). Implementing Serpent Cipher in Field Programmable Gate Arrays. *Fifth International Conference on Information Technology*, 11(17):50-372.

Symantec. (2011). Enterprise Encryption Trends Study. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20111130_02 (Accessed 26 January 2016).

Thawte. (2013). History of Cryptography. *An Easy to Understand History of Cryptography*. Available: http://book.itep.ru/depository/crypto/Cryptography_history.pdf (Accessed 25 January 2016).

The Organisation for Economic Co-operation and Development. (2009). Competition and Regulation in Auditing and Related Professions. *DAF/Comp*, (19):1-274.

Vijavan, J. (2013). *Encryption: still the best way to protect data – despite NSA*. Available: http://www.computerworld.com/article/2484714/security0/encryption-still-best-way-to-protect-data----despite-nsa.html (Accessed 16 June 2015).

Villanueva, JC. (2015). *An Introduction to Stream Ciphers and Block Ciphers*. Available: http://www.jscape.com/blog/stream-cipher-vs-block-cipher(Accessed 10 March 2016).

Zhou, H. (2015). Trusted Computing Encryption Model Based on XTR Public Key Cryptosystem. *Journal of Computational Information Systems*, 11(12):4465-4472.

Zohrabi, M. (2013). Mixed Methods Research: Instruments, Validity, Reliability and Reporting Findings. *Theory and Practice in Language Studies*, 3(2):254-262.

UNIVERSITY OF JOHANNESBURG

APPENDIX A

RESEARCH QUESTIONNAIRE

Statement of participation

Research topic: The effectiveness of encryption methods in mitigating information technology security risks. I hereby voluntarily grant my permission for participation in the study as explained to me by the covering letter. The nature and objectives of the study have been thoroughly understood. I also understand my right to choose whether to participate in the study or not and that the information completed by me will be handled as confidential.

Signed _____Date _____

Researcher _____ Date _____

UNIVERSITY OF JOHANNESBURG

SECTION A: Demographical Questions

1. Job title *(e.g. IT Security Manager)*

_____

2. The key tasks that you are responsible for in your position *(e.g. review IT security policies)* _____

_____

3. The highest academic qualifications that you have obtained *(e.g. Matric, Diploma, B Com etc.)* _____

4. Do you hold any professional qualification(s), e.g. CISA, CISM, CRISC? If yes please specify the qualification(s) in the space provided below:

_____

5. Are you a member of a professional body, e.g. IIA, ISACA? If yes, specify the professional body you are affiliated with in the space provided below:

_____

6. Please specify the number of years of experience you have in IT Security *(please indicate the amount of years of experience as a numerical value in the space provided below e.g. 3 years)*

_____

UNIVERSITY OF JOHANNESBURG

SECTION B: Symmetric Encryption

Please rate the effectiveness of the following Symmetric Encryption methods in practice.

Note: Symmetric Encryption uses one key for encrypting plaintext and decrypting ciphertext.

1.1 Triple DES encryption algorithm of between112 and 168 bit-key:

	Option	**Answer**
1.1.1	Highly breakable	☐
1.1.2	Least breakable	☐
1.1.3	Not breakable	☐
1.1.4	Not yet used	☐

1.2 Twofish encryption algorithm of 256 bit-key:

	Option	**Answer**
1.2.1	Highly breakable	☐
1.2.2	Least breakable	☐
1.2.3	Not breakable	☐
1.2.4	Not yet used	☐

1.3 CAST encryption algorithm of 128 bit-key:

	Option	**Answer**
1.3.1	Highly breakable	☐
1.3.2	Least breakable	☐
1.3.3	Not breakable	☐
1.3.4	Not yet used	☐

1.4 RC6 encryption algorithm of 128, 192 and 256 bit-key:

	Option	**Answer**
1.4.1	Highly breakable	☐
1.4.2	Least breakable	☐
1.4.3	Not breakable	☐
1.4.4	Not yet used	☐

UNIVERSITY OF JOHANNESBURG

1.5 SEED encryption algorithm of 128 bit-key:

	Option	**Answer**
1.5.1	Highly breakable	☐
1.5.2	Least breakable	☐
1.5.3	Not breakable	☐
1.5.4	Not yet used	☐

SECTION C: Asymmetric Encryption

Please rate the effectiveness of the following Asymmetric Encryption methods in practice.

Note: Asymmetric Encryption uses two different keys for encrypting plaintext and decrypting ciphertext.

1.6 RSA encryption algorithm of 1024 bit-key:

	Option	**Answer**
1.6.1	Highly breakable	☐
1.6.2	Least breakable	☐
1.6.3	Not breakable	☐
1.6.4	Not yet used	☐

UNIVERSITY OF JOHANNESBURG

1.7 ECC encryption algorithm of between 160 and 512 bit-key:

	Option	**Answer**
1.7.1	Highly breakable	☐
1.7.2	Least breakable	☐
1.7.3	Not breakable	☐
1.7.4	Not yet used	☐

SECTION D: Encryption Methods used by your Organisation and Clients

1.8 Please provide Symmetric Encryption methods used in your organisation:

_____

1.9 Please provide Symmetric Encryption methods used by your clients:

_____

1.10 Please provide Asymmetric Encryption methods used in your organisation:

_____

1.11 Please provide Asymmetric Encryption methods used by your clients:

_____

----END----

Thank you for your time and participation.

UNIVERSITY OF JOHANNESBURG