

**T.C.
SAKARYA UNIVERSITY
INSTITUTE OF SCIENCE**

**DEVELOPMENT OF DATA ENCRYPTION
ALGORITHM FOR DATABASE SECURITY BY
USING ASCII CODE**

M.Sc. THESIS

Sivan Sper IBRAHIM

**Department of the Institute : COMPUTER AND INFORMATION
ENGINEERING**
Thesis advisor : Prof. Dr. Ahmet ZENGİN

August 2021

**T.C.
SAKARYA UNIVERSITY
INSTITUTE OF SCIENCE**

**DEVELOPMENT OF DATA ENCRYPTION
ALGORITHM FOR DATABASE SECURITY BY
USING ASCII CODE**

M.Sc. THESIS

Sivan Sper IBRAHIM

Department : COMPUTER AND INFORMATION ENGINEERING

**This thesis has been accepted unanimously of votes by the examination committee on
06/08/2021**

Head of Jury

Jury Member

Jury Member

DECLARATION

I declare that all the data in this thesis was obtained by myself in academic rules, all visual and written information and results were presented in accordance with academic and ethical rules, there is no distortion in the presented data, in case of utilizing other people's works they were refereed properly to scientific norms, the data presented in this thesis has not been used in any other thesis in this university or in any other university.



Sivan IBRAHIM

24.06.2021

ACKNOWLEDGEMENT

First of all, thank God. I am deeply thankful to Sakarya University for giving me such a great opportunity to complete my Dissertation on “ Development of data encryption algorithm for database security by using ascii code ” and also their valuable guidance. I extremely thankful to Prof. Dr. Ahmet ZENGIN for his extreme support in preparing the thesis and guiding me. I am thankful to him again and again for his valuable time and to share his extra ordinary knowledge with me. I also express my indebtedness to my parents and my wife they blessings and support always helped me to face the challenges ahead.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	i
TABLE OF CONTENTS	ii
LIST OF SYMBOLS AND ABBREVIATIONS	iv
LIST OF FIGURES	v
LIST OF TABLES	vi
ÖZET	vii
SUMMARY	viii
CHAPTER 1.	
INTRODUCTION	1
CHAPTER 2.	
BACKGROUND AND LITERATURE	4
2.1. Database	4
2.2. Threats Of Database Security	6
2.3. Database Security Measures	7
2.4. Data Encryption	8
2.5. Ascii Cod	11
2.6. Cryptography	12
2.7. Need For Cryptography	13
2.8. Security Analysis Of Algorithms	14
2.9. Types Of Attacks On Cryptography	15
2.9.1. System attacks	15
2.9.2. Data attacks	17
2.10. Types Of Cryptography Algorithm	17
2.10.1. Symmetric key encryption	17

2.10.1.1. Symmetric algorithm in past	19
2.10.1.2. Blowfish	21
2.10.1.3. Data encryption standard.....	22
2.10.1.4. Triple data encryption.....	23
2.10.1.5. Advanced encryption standard	24
2.10.2. Asymmetric key encryption	25
2.10.2.1. Rsa algorithm	26
2.10.3. Hash function	27
 CHAPTER 3.	
LITERATURE REVIEW	28
 CHAPTER 4.	
METHODOLOGY	31
4.1. Practical Section	35
 CHAPTER 5.	
RESULT AND DISCUSSION	38
 CHAPTER 6.	
CONCLUSION	42
 REFERENCES	43
RESUME	47

LIST OF SYMBOLS AND ABBREVIATIONS

CDB	: Centralized database
DDB	: Distributed database
DBMS	: Database management system
DBA	: Database administrator
EPA	: Excessive privilege abuse
LPA	: Legitimate privilege abuse
MAC	: Mandatory access control
RBAC	: Role-based access control
ABAC	: Attribute-based access control
DLE	: Database-level encryption
CT	: Cipher text
PT	: Plain text
TDES	: Triple data encryption standard
DES	: Data encryption standard
AES	: Advanced encryption standard
RSA	: Rivest shamir adleman
ASCII	: American standard code for international interexchange
CPA	: Chosen plaintext attack
CCA	: Chosen cipher text attack
NIST	: National institute of standards and technology

LIST OF FIGURES

Figure 2.1. Control measures to protect DBs.....	8
Figure 2.2. Levels of encryption	9
Figure 2.3. Cryptographic model	13
Figure 2.4. Normal flow of information	15
Figure 2.5. Interrupted data flow	15
Figure 2.6. Interception attack	16
Figure 2.7. Modification of data	16
Figure 2.8. Fabrication system attack	16
Figure 2.9. Symmetric key encryption.....	18
Figure 2.10. Blowfish algorithm.....	21
Figure 2.11. Data encryption standard structure	23
Figure 2.12. Advanced encryption standard structure	25
Figure 2.13. Asymmetric key encryption.....	26
Figure 2.14. Key generation in RSA algorithm	27
Figure 2.15. Hashing algorithm	27
Figure 4.1. Equation diagram.....	31
Figure 4.2. Create user	35
Figure 4.3. Login form.....	36
Figure 4.4. Login form.....	36
Figure 4.5. Speed test form	37
Figure 5.1. Frequency of the encryption text	39
Figure 5.2. Frequency of the decryption text	39
Figure 5.3. Encryption time vs. file size for DES, 3DES, AES, Blowfish, RSA	40
Figure 5.4. Decryption time vs. file size for DES, 3DES, AES, Blowfish, RSA	40
Figure 5.5. Encryption and decryption time	41

LIST OF TABLES

Table 2.1. Simple substitution cipher.....	19
Table 2.2. Play fair cipher example with keyword domestic.....	20
Table 4.1. Examples of encrypting text (1) in equation (1)	32
Table 4.2. Examples of encrypting text (2) in equation (1)	32
Table 4.3. Key (1) generating equation.....	33
Table 4.4. Key (2) generating equation.....	33
Table 4.5. Encrypting procedure.....	34
Table 4.6. Decrypting procedure.....	34
Table 5.1. Data encryption in our system	38

ASCII KODU KULLANARAK VERİTABANI GÜVENLİĞİ İÇİN VERİ ŞİFRELEME ALGORİTMASI GELİŞTİRİLMESİ

ÖZET

Anahtar Kelimeler: Kriptografi, Veri Şifreleme, Veri Şifre Çözme, Düz metin, Şifreleme metni

Şu anda, birçok insan yavaş yavaş yeni ilerleme ve gelişime doğru ilerleyen teknolojileri uygulamaktadır. Dahası, çoğumuz iş yönetimimize yardımcı olmak için veritabanı sistemlerini kullanıyoruz; veri tabanı, işimizi veya kişisel bilgilerimizi içerir ve bu da yıkıcı elektronik saldırılar nedeniyle verilerimizi kaybetme riskini artırır. Sonuç olarak, veritabanlarını elektronik saldırılardan ve veri ele geçirmelerinden korumak çok önemlidir ve verileri tanımlamanın bir yöntemi, elektronik saldırılar sırasında verilerimizden hiçbir fayda elde edilmemesi için çeşitli algoritmalar kullanmaktır. Bu yazıda, verilerin Şifrelenmesi için oluşturduğumuz belirli bir formülü açıklıyoruz. Veriler Ascii Kodu kullanılarak şifrelenir. Ayrıca ana formülde üç anahtar kullandık. Bu formül sayesinde veritabanına kaydettiğimiz her veri şifrelenecektir. Veriler Metin veya sayı olabilir. Ve önceki üç anahtarla başka bir koordinatör kullanarak, verileri orijinal tarzımıza göre işleyebiliriz. Formül, verilerin makul bir hızda şifrelenmesiyle aynı veri boyutunu elde etmemizi sağlayacak şekilde veri boyutuna ve kayıt hızına odaklanır.

SUMMARY

Keywords: Cryptography, Data Encryption, Data Decryption, Plain text, Cipher text

Currently, many people apply technologies, which are gradually moving towards new progress and development. Moreover, many of us utilize database systems to assist our work management; the database contains our work or personal information, which increases the risk of losing our data due to disruptive electronic attacks. As a result, protecting databases from electronic attacks and data seizures is crucial, and one method of identifying data is through several algorithms so that no benefit is taken from our data during electronic attacks. In this thesis, we explain a particular formula we created for the Encryption of data. The data is encrypted using Ascii Code. Also, we used three keys in the main formula. Because of that formula, each data we save in the database will be encrypted. The data can be Text or number. And through using another coordinator with the three previous keys, we can render the data to our original style. The formula focuses on data size and recording speed in such a way that we get the same data size as when the data is encrypted at a reasonable speed.

CHAPTER 1. INTRODUCTION

A database is an organized group of data organized to facilitate access, management and updating. In easy words, you can say, a database is a site where data is stored.

The optimal similarity is the bookshop. The bookshop includes a large assembly of books of dissimilar kinds, the bookshop in this place is database also books are the data [40]. Now the use of databases in business, management, science and other fields has increased greatly, and we carry many of our data, personal information, With the increasing use, the cyber-attacks have also increased, which will capture the data and information available to us, so we need to pay more attention to protecting our databases. Database security implies the dissimilar steps firms apply to make sure its databases are saved from inside also outside risks.

Database security contains saving the database per se, the data includes. one of the techniques used to protect databases is cryptography [41].

Several articles have been written in the literature. For instance, authors of [24] conclude that Databases are a preferred target for hackers because of their sensitive and valuable information. A database can be hacked in a variety of ways. A database should be protected from various types of threats and risks.

In this thesis, solutions to most of the attacks are identified, although some solutions are beneficial while some are only momentary. In [5], the writer measured cipher algorithms (AES, DES, 3-DES, and Blowfish) to various data dimensions and encryption period for two separate devices, a Pentium-4, 2.4 GHz, and a Pentium-II 266 MHz in EBC and CFB Mode. The writer decided Blowfish is the quickest afterward DES as well as Triple DES, also CFB needs longer compared to ECB cipher block mode.

The encryption algorithm proposed by the author in [19] is dependent on the ASCII value of the message to be encoded. This algorithm requires a key that has the same length as the letter. This key is encrypted and utilized in the encryption and decryption processes. This device requires the user to input the key. If the message is longer than the device allows, the recipient is asked to input a key identical to the range of the letter. It makes it hard task for the user to input a large key. Another disadvantage of this algorithm is that it takes longer to execute. So, these are the two deficiencies of the current algorithm.

Different widely known special key algorithms, for example DES, 3DES, AES, as well as Blowfish, are explored by the author in [7]. They were put to the test, and its efficiency was measured through encrypting input folders of various points and dimensions. To compare performance of the algorithms, they were evaluated on pair separate hardware stages. They did the performance on pair separate apparatus: a P-II 266 MHz machine as well as a P-4 2.4 GHz machine. When compared to, other algorithms the results revealed that Blowfish performed exceptionally well. It was also discovered that AES outperformed 3DES and DES.

Nowadays, due to the overuse of technology, particularly in the fields of communication, commerce, education and etc., attacks have also increased, including attacks on database systems and the seizure of personal and private data. In this context, our goal is to focus more on protecting our data from database attacks by creating a data encryption algorithm by Ascii code. Considering the strength of the keys, the size of data and the speed of encrypt and decrypt data, which is due to its comparison with other common cryptographic algorithms.

We created the formula using four other subformulas and three keys in a way that each key is encrypted through those subformulas and then used in the main formula with ASCII code to strengthen the protected side of our formula and at the same time in the formula we reached the result that the size of the original data and the encrypted data are equal.

Our work will be organized as follows: section 2 consists of giving overview of Cryptography. We will also describe the data encryption. Section 3 describes our algorithm and practical. In section 4, we present and discuss the results of test our algorithm and compare with other common algorithms.

CHAPTER 2. BACKGROUND AND LITERATURE

2.1. Database

Since the 1960s, DBSs were created and have become remarkably crucial to dissimilar firms so as to cause the data better coordinated as well as being accessible to per consumer. A database (DB) is the collection of data which are connected in pairs and serve in place of information which has the ability to be recorded as well as containing indirect implication. Databases are categorized based on their architecture: concentrated DB (CDB) alternatively disseminated DB (DDB). A primary distinction amid CDB and DDB is the CDB saves whole statistics and information in a a mere place, however the DDB saves various parts of DB inside many corporeal places [35].

Regarding the CDB, a interference in a mere site leaves the complete structure inaccessible for any consumer, however regarding the DDB, consumers have the ability to visit other DB locations. DBS can be built using different data structures, including comparative patterns, categorized patterns, as well as patterns towards object. The mentioned various DB patterns contain numerous personal alternatively delicate documents, like data of credit card, data about medicine, as well as pupil history that have to be kept secure against disallowed use. As well as intensified risks for DBs, the necessity for maintaining dataprivacy coupled with secrecy has arisen as a safeguard against any threats.

Many approaches have appeared to secure data, and three requirements must be fulfilled to achieve this goal. There are the following: confidentiality, integrity, and availability. Confidentiality is the use of a set of rules to prohibit an unlicensed person from accessing records. The term "integrity" refers to the assurance that the data is not

subjected to any alteration or degradation [35]. Availability ensures that the customer has consistent and timely access to the information.

The lack of any of these requirements endangers the database. Since the mid-1970s, DB system security has gained a great deal of interest, beginning with entry restriction patterns to DB order that is regarded one among the early safety approaches for DB safety. Entry restriction is a system that checks a consumer's privileges in the face of a catalogue of authorization to ensure data integrity and confidentiality. Authorization is the method of defining which database operations a consumer has the ability to carry out also what data the consumer has the ability to enter. One more tool for verifying the consumer's persona is verification that is first step in accessing the database [35].

Also, subsequent to verifying the consumer within the figure, the database management system (DBMS) contains several mechanisms, for example inspection inquiry coupled with display, which keep the data safe from disallowed interactions. An inspection inquiry is a process which is considered like records belonging to activities performed by a particular person in the database. As a result, if an illegal procedure is carried out, the database administrator (DBA) will investigate the account number which was chosen for carrying it out. A sight approach is a digital table which is generated through performing comparative exercises on the base table [26].

The approach has the capacity to enable a user for accessing a portion of a relation while the user cannot directly reach the relation. Data secrecy may as well get protected through employing encryption methods which may be used on the figure. encryption data applying a cipher makes it indecipherable for other consumers apart from the person having the material to decode the data [16]

2.2. Threats Of Database Security

Risks are either problem or activity which may negatively impact DB protection, and they can be deliberate or unintentional [26]. The following are some of the most widespread threats to database security:

1. **Privilege Abuse:** We have two types of Privilege Abuse: Excessive Privilege Abuse (EPA) as well as Legitimate Privilege Abuse (LPA). EPA occurs while consumers get control of entry rights for the database which outweigh its task responsibilities; the mentioned advantages can be abused for harmful purposes [22]. The permitted user's use of legal DB privilege for harmful purposes is referred to as LPA [22].
2. **Privilege Elevation:** If the database has a loophole, an attacker might be able to manipulate it to change the advantages entry against typical consumer to manager consumer [22].
3. **SQL Injection:** SQL Injection occurs while an assailant enters sequences of illegal SQL statements into a vulnerable SQL datameans. applying SQL injection, assailants can receive full entry for the whole database [27].
4. **Platform Vulnerabilities:** Vulnerabilities in performing systems as well as whatever external assistances enabled on a DB server may cause DB harm for instance disallowed entry, rejection of assistance, alternatively dataexploitation [27].
5. **Weak Audit Trail:** Audit trails are designed to save per consumer's actions inside the database. As a result, the insecurity of an audit trail endangers the organization's databases [16].
6. **Rejection of Assistance:** It is a threat which inhibits permitted consumers against entry for the DB. It poses the danger to every company [16].

7. **Weak Authentication:** Weak verification can enable hackers for employing techniques for example (community engineering as well as violent strength) for hacking legitimate consumers' usernames as well as secret code to subsequently enter the database [27].
8. **Backup Data Exposure:** Since backup DB storage media is rarely secured from any threat, several conditions of safety violations involved stealing hard disks as well as backup tapes. [27]

2.3. Database Security Measures

Implies methods which protect database against disallowed individuals, on purpose attacks, data leakage, also those who hack [26]. It covers a wide range of problems, including lawful, moral, regulation, as well as order-connected concerns. Database safety is defined like a complex stage which every company ought to strengthen to perform their actions smoothly also effectively. Any good company demands that the security and privacy of its data be saved from disallowed entry also vicious alternatively unintended alteration [16].

Data security is achieved through various sides of a data control scheme (DBMS). DBMS is a collection of implementations that handles the data stored inside a database also aids in data organization for a better performance [17].

To minimize risks, all DBMSs have security strategies developed for these purposes [18]. Many security mechanisms have been developed to secure databases.

The four main security mechanisms that are applied to protect DBs from attacks are as follows: entry restriction, disruption management, flow management, also figure encryption.

Figure 2.1 depicts these monitoring steps. As previously said, entry management is a procedure which ensures data security by comparing the user's privileges to a list of licences.

The mentioned licences are managed using a Discretionary Access Control (DAC) approach, a Mandatory Access Control (MAC) approach, a Role-Based Access Control (RBAC) approach, alternatively an Attribute-Based Access Control (ABAC) approach (ABAC). When individuals only get entry to analytical or synopsis data, the inference control prohibits them from inferring sensitive information that are not allowed for reciting.

Flow control guarantees which no unauthorized users can access the records. Encryption (as previously stated) considered as an act of transforming data applying a cipher to cause it illegible for all consumers but the persone having an entrance to decode the figure[26].

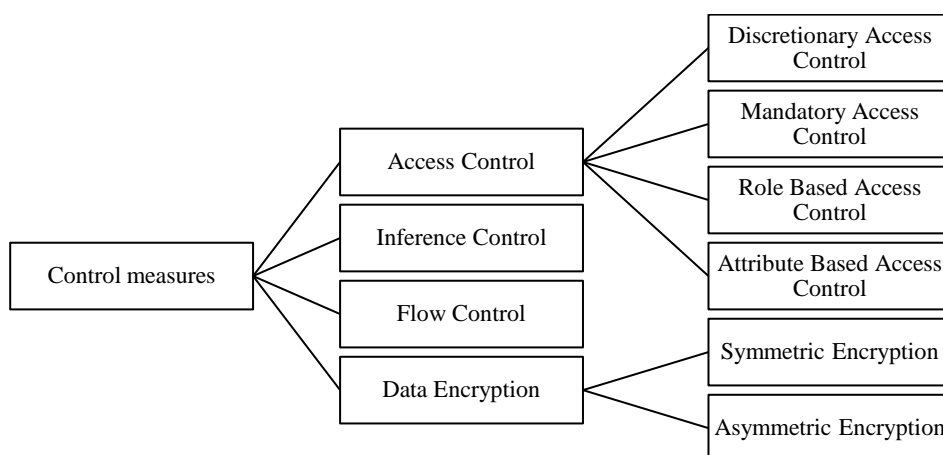


Figure 2.1. Control measures to protect DBs

2.4. Data Encryption

As data is encrypted with a cipher, it becomes unreadable to the total of consumers apart from people having the entrance for decoding the data [16]. despite the fact that hackers compromise entry restriction procedures, the encryption entries are still required for decoding the data [31].

Encryption stages relies on the algorithm as well as the entrance applied to encrypt figure. There are two kinds of encryption: ordered encryption as well as deformed encryption. Encryption has the capacity to be performed at three dissimilar stages, like seen below. Figure 2.2. depicts them:

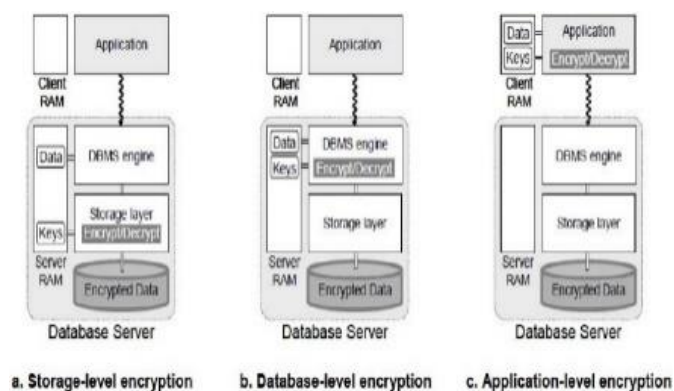


Figure 2.2. Levels of encryption

1. **Storage-Level Encryption:** storehouse-level encryption encrypts data inside the storehouse component, protecting it, for instance, against storehouse television stealing). It is ideal for encrypting folders alternatively whole folders within a performing order circumstance. Storage-level encryption has the benefit of being transparent from a database standpoint, preventing any updates to the current applications. However, as the storehouse component is unaware of objects of database as well as order, the encryption technique is not likely to be linked to consumer rights ,for example, applying different encryption entries for different consumers) or data delicacy.

As a result, choosy encryption – that is, encrypting merely database parts for reducing encryption elevated –restricted to the folder granularity. Furthermore, discriminatingly encrypting folders is unsafe as no copy of confidential data can be left unencrypted, for instance, in log folders, momentary files, and so on. [12].

2. **Database Encryption (DLE):** database-level encryption secures data since it is being put into alternatively extracted relative to a database. Thus, the

encryption technique could get integrated into structures of the database as well as getting linked to data delicacy alternatively consumer rights. Discerning encryption is feasible also could be conducted at different levels of granularity, including rows, columns, as well as tables. It may also get linked to particular logical requirements (for example, encrypt wages greater than 10K€ per month).

For both methods, on the database server at duration data is decrypted. In this way, on the server-side, the encryption entries have to be transferred alternatively held coupled with encrypted files, offering a poor level of security in opposition to the server administrator and an attacker impersonating the administrator. hackers may also tail the histroy plus find encryption keys or plain text data [12].

3. Application-Level Encryption: Application-level encryption transfers the encryption/decryption mechanism toward the data-generating devices. Encryption is therefore conducted in the program which brings the data to the network. The data is transferred encrypted, thereby normally kept and recovered encrypted, to be eventually decrypted inside the application.

Since the keys never ought to depart the application side, this technique has the advantage of separating encryption keys from the encrypted data contained in the database. But, to implement this approach, programs must be modified. Furthermore, relying on the encryption granularity, the program could be required to retrieve a greater collection of data than that given to the utilizer, therefore creating a security leak. certainly, the utilizer (or other hacker obtaining entry to the computer that the program works) can access the program and obtain illegal entry to data Finally, such a technique results in output overheads (indexes on encrypted information are purposeless) also prevents the employment of progressive database workability like saved formula (i.e., code saved within the DBMS that could be exchanged and used

via multiple programs) as well as triggers on encrypted data (i.e., code fired whilst several information within the database are added).

Application-level encryption has the most flexibility in regards to granularity and key control since the encryption granularity and encryption keys can be selected based on application logic [12].

2.5. Ascii Code

American Standard Code for Information Interchange (ASCII) is a symbol-representation code which applies data. Per letter is designated between 0 and 127. A separate data is designated to per capital as well as small letter.

Like seen in the ASCII mentioned below table, letter A is designated the digit number 65, however letter an is designated the decimal number 97. ASCII code returns to the teletypes times as well as mechanic-like printers, but it antecedes the Internet. Management codes for ASCII decimal data starting from the limitation of 0 to 31 are not anymore largely available.

However, in case you want to attempt to play alongside associations procedures, you can view the restriction codes in application. - of the restriction codes is explained in the ASCII Control Codes table. The entries you click alternatively correspondences are obtained like a sequence of data while a device delivers consequences. letters that you wrote or made are symbolized through these data. As the typical ASCII limitation is between 0 and 127, merely 7 bits or 1 byte of information is required. to give the string cactus.io like ASCII, for example, it could be 99 97 99 116 117 115 46 105 111. Just bits as well as bytes are understood by microprocessors. All is a series of pieces to it.

2.6. Cryptography

Cryptography is a method of protecting data from unauthorized entry. It is made up of two major parts:

1. Encryption algorithm.
2. Key.

Different keys may be used for encryption in some cases. Cryptographic algorithms such as DES, AES, TDES, Blowfish, and Cryptosystem are present on the market. The strength of these encryption algorithms is determined by the strength of their keys. Strong encryption algorithms and key management techniques are often helpful in achieving data security, authentication, and integrity while reducing device overheads. The longer the key, the more time it takes to break the code, and the hacker have a harder time detecting the cryptographic model. There are two types of cryptography:

1. Symmetric Cryptography.
2. Asymmetric Cryptography.

In symmetric cryptography, the entry applied for encrypting as well as decrypting the letter is the same, however with regards to asymmetric cryptography, the entries applied to encryption as well as decryption are special. Asymmetric algorithms are more sluggish compared to symmetric algorithms, though they have high degree of protection. There are a few key terms in cryptography, which are listed below:

1. Plaintext: This is the text that has to be encrypted [2].
2. Ciphertext: This is the text that has been encrypted. Ciphertext [6] is the text that results from encoding data with the aid of an entry.
3. Key: A value alternatively word which is applied for encrypting or decode simple letters or cipher text [1].

4. Encryption: It is the stages of transforming data to coded format using a key [3].
5. Decryption: Decryption is a process of returning encoded data into its primary shape [1].
6. Crypto Analyst: A crypto analyst is a specialist in deciphering and decoding codes [2].

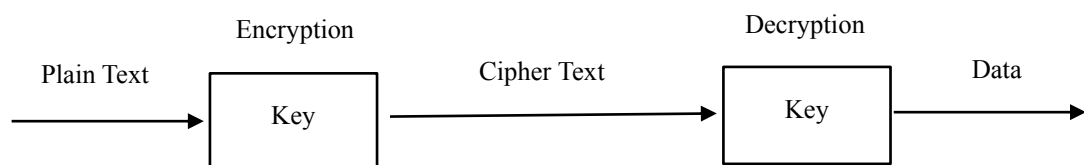


Figure 2.3. Cryptographic model

2.7. Need For Cryptography

Nowadays, cryptography turned into requirements to the whole of the firms. Data safety is a critical element in a firm for maintaining the data risk-free against different rivals. It as well assists in making sure the confidentiality of a consumer with relative to opposites. Currently, codes are not thought to be much dependable regarding this duty as it is effortless for finding out codes because of the limited scope. Furthermore, in case the scope of code is tiny a violent strength exploration may be utilized to break it [2].

Accordingly, in order for preserving our data different algorithms have been formed. It assists for carefully attain bank accounts, electronic reposition of financial supports as well as a lot of diurnal life implications.

2.8. Security Analysis Of Algorithms

With regards to E-Commerce, various algorithms are applied to cryptography. The total algorithms provides various levels of security which relies on the way to show how difficult they can be to collapse.

1. In case the price needed to dismantle an algorithm is bigger compared to the price of the encrypted figure, afterwards the algorithm is considered risk-free.
2. In case the duration needed dismantling an algorithm is larger compared to the duration which the encrypted data need to stay concealed, subsequently it is risk-free as well.
3. In case the quantity of data encrypted alongside a mere key is smaller compared to the quantity of data required to dismantle the algorithm, it is considered risk-free. DATA (Plain Text) Plain Text changed to multiple Cipher Text applying key Multiple Cipher Text changed back to Plain Text applying identical key DATA (Plain Text).
4. Algorithm is risk-free in case it is hard for finding security key as well as discover the primary context. In that state, just a single time pad is durable in a cipher text merely hack, plainly via attempting each feasible keys one at a time also via inspecting if the occurring plain text has meaning. This is called a brute force attack.

Cryptography is further troubled with crypto systems which are computationally impracticable to crack. each algorithm is considered as computationally safe when it cannot be hacked with accessible facility. A favorable property of each encryption algorithm is the tiny calteration in plain text or the key should generate important alter in cipher text. Like impact is recognized as accessible impact. The more the avalanche the algorithm impacts, the greater the safety. Crypto inspection is the investigation of retrieving the plain text in unaccompanied by the availability to the key. this might

discover weakness as well in a crypto system which recognizes patterns that can be advantageous in getting to know to the previous results.

2.9. Types Of Attacks On Cryptography

We have fundamentally two kinds of attacks. First system, second data:

2.9.1. System attacks

1. Overall a surge of data is there from a starting point to a target. The assaults that are on the surge of data are recognized like order assaults. The major threats on safety are mentioned as follows:

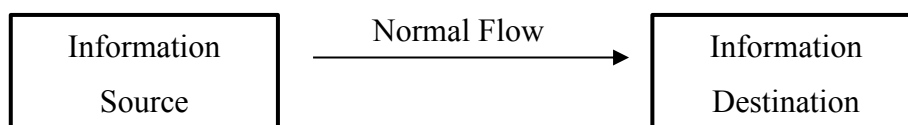


Figure 2.4. Normal flow of information

2. Interruption: refers to an assault on supply accessibility. In case the information surging via starting point to target turns into incredible alternatively unconsumable [8].

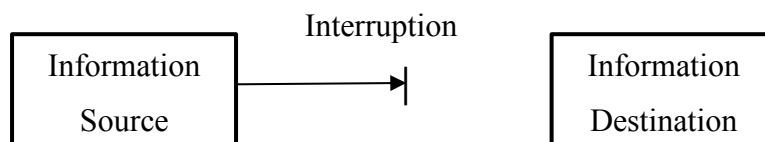


Figure 2.5. Interrupted data flow

3. Interception: It's a violation of the system's confidentiality. In this assault an unapproved party moreover contains the entry to a pattern. A human, program as well as computer might be the unapproved side [1].

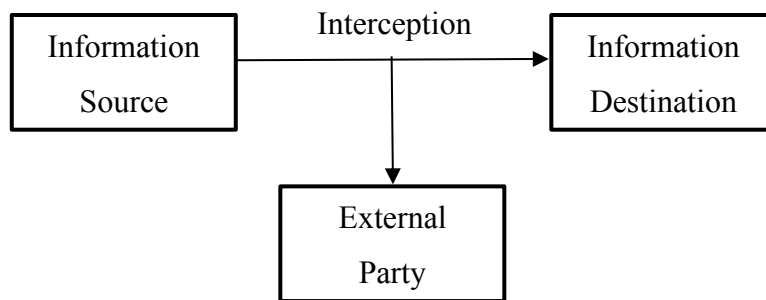


Figure 2.6. Interception attack

4. **Modification:** refers to an assault on order incorporation. within this assault an unapproved side does not only contain the entry into a benefit however contains the capability to change it [15].

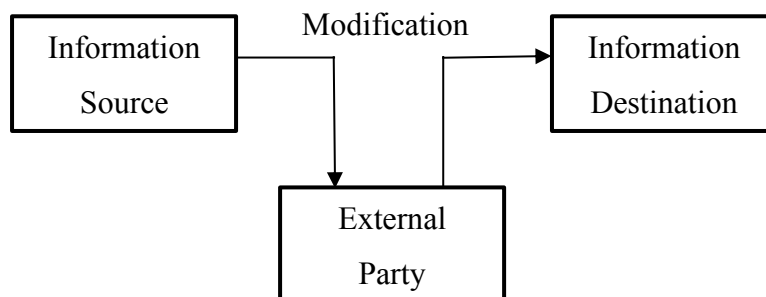


Figure 2.7. Modification of data

5. **Fabrication:** refers to an assault on order accuracy. Within this one an unapproved side puts counterfeit things to the order [1].

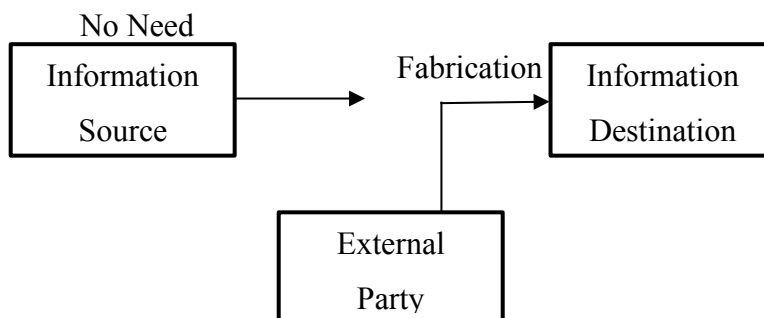


Figure 2.8. Fabrication system attack

2.9.2. Data attacks

A strived crypto dissection is recognized like a risk. The data amount which decoder can derive from the cryptosystem plus could be splited to five types of decryption which explained below:

1. Cipher text only threat: The crypto dissection includes cipher text of some texts as well as every the encrypted text applying the identical encryption algorithm. After that, task is for retieving the plain text or the key applied for encrypting the texts. According, for decrypting further section of texts encrypted via the assist of the keys which were used [1].
2. Known Plaintext threat: Crypto dissection look for having pairs of recognized plain text as well as cipher text. next task is to have the key applied for encrypting the texts an algorithm for decrypting texts [2].
3. Chosen Plaintext Attack (CPA): Crypto dissection does not merely posses the cipher text, it also certains sections of selected plain text as well. invader is recognized to be located at encryption place for performing the threat [1].
4. Chosen cipher text attack (CCA): this crypto dissection have the chosen cipher text and plain text which are encrypted using the personal key. Although, this just can enter an encryption device [9].

2.10. Types Of Cryptography Algorithm

2.10.1. Symmetric key encryption

Private-key cryptographic algorithms are divided into stream ciphers or block ciphers depending on the way they control data. A stream cipher controls data one sign, normally a piece, in the moment whilst a block cipher encrypts data in constant- distant blocks.

Many cryptographic algorithms applied presently are block ciphers as well as stream ciphers are applied mainly through circumstances where transmitting failures are probable and performance materials are restricted like mobile phones [28].

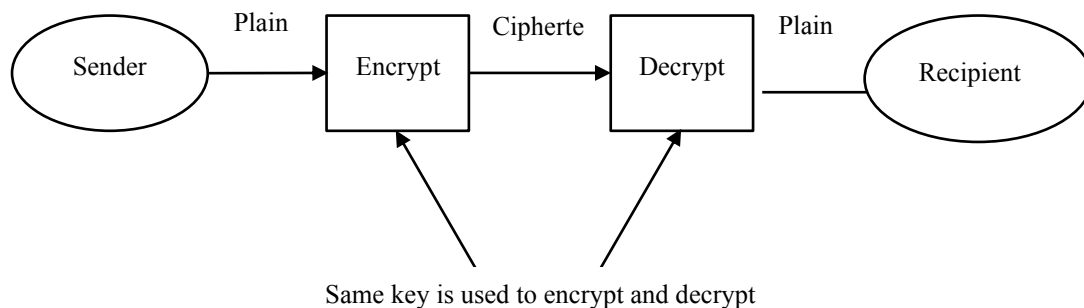


Figure 2.9. Symmetric key encryption

Symmetric key encryption method or private key encryption method includes the mentioned five ingredients:

1. Plain text: it is the initial comprehensible text or information is installed in the algorithm like input.
2. Encryption algorithm: The encryption algorithm utilizes various substitutes and transitions on the plaintext.
3. Private Key: The private key is as well input to the algorithm of encryption. The key is a useful entity of the plaintext. The algorithm would generate a various output related to particular key being applied during the moment. The precise replacements as well as transitions implemented by the algorithm rely upon the key.
4. Cipher text: it is the disorganized text generated as output. which is based on the plaintext as well as the private keys. For a specified text two dissimilar keys would generate two unlike cipher texts. The cipher text is a superficially haphazard sequence of information and, as it remains unreadable.

5. Decryption Algorithm: - it is fundamentally the encryption algorithm operate conversely, which requires the cipher text, the private key as well as generates the initial plaintext

2.10.1.1. Symmetric algorithm in past

Cipher codes as well as various old encryption algorithms have been applied all through history to avoid non allowed individuals from understanding the text. A few past algorithms:

1. Caesar Shift Cipher applied by Roman Army: Caesar Cipher is an instance of symmetric cipher. Caesar Cipher has been given the name of Julius Caesar whom applied that encryption algorithm in order to encrypt the armed forces and authority text. Algorithm

$$P = C \text{ key mod } 26 \quad C = P + \text{key mod } 26 \quad P = C \text{ key mod } 26$$
Presume key is 3 also plaintext contains ABCD therefore the cipher text would be DEFG [38].
2. Simple Substitution Cipher: it is an instance of symmetric key cryptography as well in here the transmitter as well as the recipient agree on haphazardly chosen organized characters of alphabets. Transmitter substitutes each plain text character through replacing the organization which is straight under its table however recipient on getting cipher text exchanges every other cipher text character to the correlating plaintext in the main line [38].

Table 2.1. Simple substitution cipher

PT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CT	C	F	J	L	O	B	P	R	U	V	X	Z	D	Y	W	T	G	I	M	N	A	Q	S	H	K	E

3. Play fair Cipher: Play fair cipher has originally created via Charles Wheatstone in 1854, the play fair cipher name was chosen to honor its organizers Lord play fair. The play fair cipher utilizes more than one characters in the place of single character, replacement cipher complexes the cipher text as well as makes it more difficult to predict. The play fair cipher is built on $5 * 5$ table of letters

formulated utilizing keyword. Order of play fair cipher for creating cipher text through plain text [38].

1. dissect the plain text to a couple of letters.
2. When the two letters are similar, insert filler letter x following the main letters, consequently introducing latest combination as well as maintaining as an example of balloons are going to be lx lo on.
3. when every character of simple words lie into identical line, exchange it with the character under it, alongside the high part of the column in a circular way taking after the final.
4. when the pair of the letters of the plain text lie into the identical line then replace it to the one located on the right, with the primary part of the line taking after the rear in a circular way.
5. If the two of the letters of the plain text lie into various row, replace it to the character that lies into its line and the lines taken up via different plain text.

As a result, the keyword matrix is when the keyword is local and the plain text is the key which hidden underneath the door. The table is

Table 2.2. Play fair cipher example with keyword domestic

D	O	M	E	S
T	I	C	A	B
F	G	H	K	L
N	P	Q	R	U
V	W	X	Y	Z

2.10.1.2. Blowfish

Blowfish is an asymmetric encryption algorithm, which means it utilizes the exact hidden code for encrypting and decode communications. When it comes to encryption and decryption, Blowfish is a block cipher too, which means it dissects a text to established length blocks. Blowfish has a block width of 64 bits, therefore texts that aren't a diversity of eight bytes have to be padded.

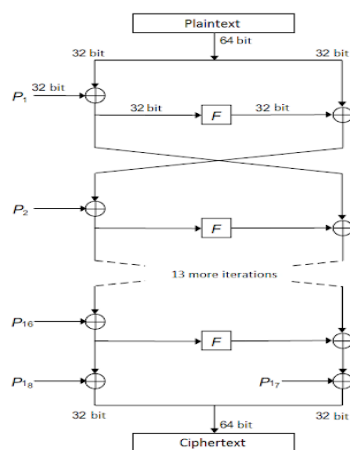


Figure 2.10. Blowfish algorithm

Blowfish contains pair elements: key-expansion as well as data encryption. In the entry enlargement stage, the inputted key is shifted to some sub key arrays complete 4168 bytes. we can see the P range which is eighteen 32-bit boxes, also the S-boxes which are four 32-bit lines alongside 256 entries for every one of them.

When passing the beginning of strand, the original 32 bits of the key are XORed alongside P_1 (the initial 32-bit box in the P-array). The next 32 bits of the key are XORed plus P_2 , etc. To the point where all 448, or less, key bits have been XORed Cycle via the entry bits through going back toward the initials of the key, till the whole P-array has been XORed alongside the entry. Encrypt all zero-string applying the Blowfish algorithm, implementing the changed P-array above, for receiving a 64-bit block. Substitute P_1 with the primary 32 bits of output, also P_2 and the second 32 bits of output (from the 64-bit block). Apply the 64-bit output as input back into the

Blowfish cipher, to receive a new 64-bit block. Substitute the following prices in the Parry and the block.

Do the same thing with each value in the P-array and every S boxes orderly. Encrypt the all zero-string applying the Blowfish algorithm, applying the changed P-array which mentioned before, for receiving a 64-bit block. Substitute P1 to the primary 32 bits of output, and P2 to the second 32 bits of output (from the 64-bit block). Apply the 64-bit output as input back into the Blowfish cipher, for receiving a new 64-bit block. Substitute the following prices within the P-array with the block. Do the same regarding each value in the P-array as well as every S boxes orderly [29].

2.10.1.3. Data encryption standard

The Data Encryption Standard (DES) is a symmetric entry algorithm progressed at the beginning of 1970s at IBM. The Data Encryption Standard is the largest largelyutilized cipher. It was formed in 1977 by IBM also it has the capacity tostand against all endeavors at cryptanalysis. The Data Encryption Standard is a square shape that implies a cryptographic entry also figuring are related to a fragment of data all alongin contrast with a single fragment immediately.

For having a simple word letter scrambled, DES groups it to 64-bit fragments. Eachbit is encrypted applying the confidential entry for producing a 64-bit output cipher words through an approach regarding phase as well as replacement. The process contains 16 adapts as well as has the ability to maintain continuing in four different patterns, alternatively deforming fragments especially. Decoding is fundamentally the other way round of encryption, following the exact strides still completing the demandt where the entries are related. The amount of likely entries relies on the breadth of the entry also the credibility—of this type of strike. DES applies a key of 64-bits, eight of the bits are applied regarding fariness inspections, effectively constricting the approach to 56-bits. Hereafter, it needs a significant of 2^{56} , or 72,057,594,037,927,936, efforts place the accurate entry. It splits the data to get

encrypted to a special series of blocks of 64-bit furthermore applies a key of 56-bit to perform a sequence of transformations in terms of mathematics to it.

We have different varieties of the DES algorithm, nsuch as cipher block altering, where each block of data utilizes XOR function alongside the last block to an extent prior to encryption, also however, in triple-DES, the method of DES is utilized thrice in the sequence. The goal of the DES algorithm is to provide a customary style for obtaining private and disordered data. In this procedure, encryption plus decryption procedure apply the identical entry [23].

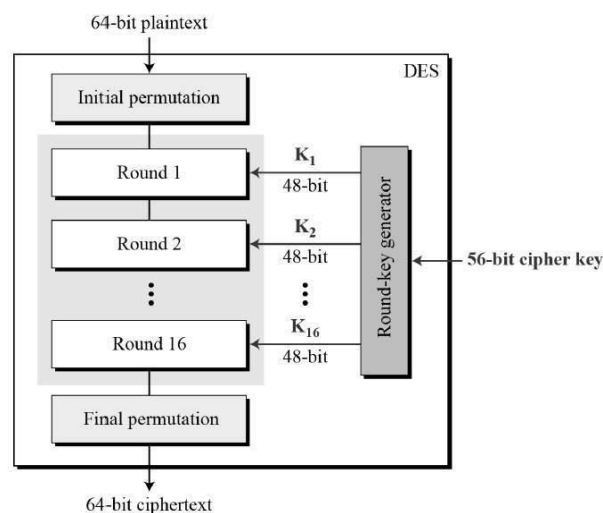


Figure 2.11. Data encryption standard structure

2.10.1.4. Triple data encryption

3DES alternatively the Triple Data Encryption Algorithm (TDEA) was progressed for solving the apparent defects in DES deprived of forming a total novel cryptosystem. Data Encryption Standard (DES) applies a 56-bit key also cannot be expected adequate for encrypting delicate figure. 3-DES plainly expands the entry dimension of DES by utilizing the algorithm thrice in series accompanied by three various entries. The mixed entry dimension is therefore 168 bits (3 times 56). TDEA includes utilizing three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) pattern, which is, the simple words is encrypted alongside K1, afterwards decrypted with K2, and

subsequently encrypted one more time alongside K3 [23]. The standards identify three entry choices:

Choice one the favorable choice, implements three reciprocally detached keys ($K1 \neq K2 \neq K3 \neq K1$), which provides key space of $3 \times 56 = 168$ bits.

Choice two performs two reciprocally individual entries as well as a third entry which is identical like the main key ($K1 \neq K2$ and $K3 = K1$). which provides key space with $2 \times 56 = 112$ bits.

Choice three is a key array of thrice similar keys ($K1 = K2 = K3$). This one is equal with DES Algorithm. In 3-DES the tripple iteration is utilized for rising the encryption stage as well as customary duration. It is a recognized truth 3DES is more sluggish compared to the rest of block cipher techniques [23].

2.10.1.5. Advanced encryption standard

In the 1990s, the United States National Institute of Standards and Technology (NIST) performed a contest to form a replacement regarding DES. The victor, Rijndael, was published in 2001. It caused the RSA algorithm the novel Advanced Encryption Standard (AES). AES includes three square numbers, AES-128, AES-192 also AES-256. every number encodes and decodes information in squares of 128 bits applying cryptographic keys of 128-, 192-, also 256-bits, freely. (Rijndael was meant to deal with additional fragment dimensions as well as entry spreads, though the advantage was not the main point in AES.) Symmetric algorithms applies the widespread private entry for decryption as well as encryption, accordingly the deliverer and obtainer ought to be conscious also be capable for applying the identical private entry..

Each individual entry breadth is assessed sufficiently for ensuring organized data needing 192-alternatively 256-bit key breadth. We have 10 cycles of 128-bit keys, 12 cycles regarding 192-bit keys, also 14 cycles regarding 256-bit keys (a round is some base measures which contain changing, combining, also replacement of the input simple

words as well as altering it for the final yield of cipher text). Rijndael combines up the SPN pattern through involving Galios implementations of the field in each circle. Somehow alike to arithmetic implementations of RSA modulo, the field implementations of Galios generated gibberish, however could be reversed in terms of mathematcs. AES contains Safety, moreover, including a connection between duration and price [34].

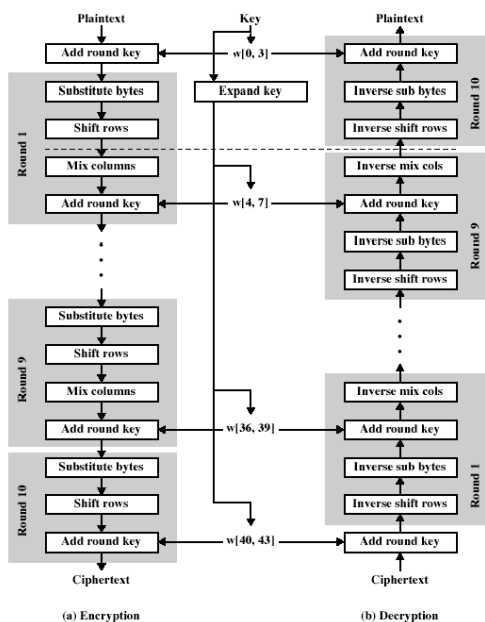


Figure 2.12. Advanced encryption standard structure

2.10.2. Asymmetric key encryption

In asymmetric device two entries are applied: confidential entry as well as general entry. General entry is utilized to encrypting also confidential entry is applied to decrypting. However the major issue regarding general entry encryption is it depends on functions regarding mathematics. Asymmetric encrypting methods are approximately 1000 times more sluggish compared to symmetric methods as they need superior mathematical preparing strength The sample of asymmetric entry algorithm is RSA algorithm that is clarified as follows [28]:

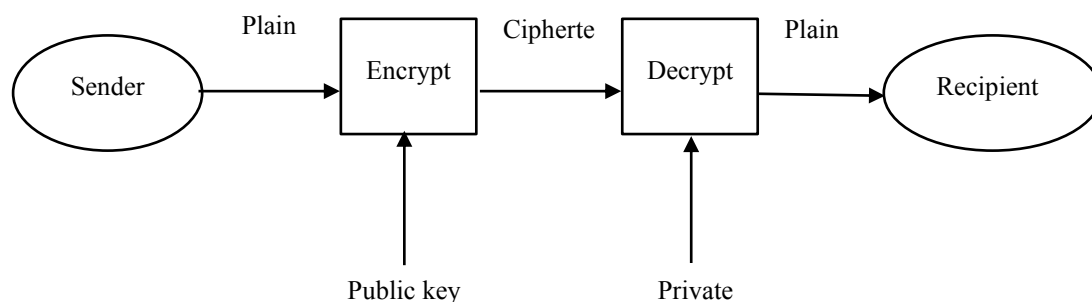


Figure 2.13. Asymmetric key encryption

2.10.2.1. Rsa algorithm

creators of RSA algorithm are Ron Rivest, Adi Shamir, and Leonard Adleman. They progressed RSA in 1977. It generally applies in different implications such as Internet Browsers and so on. It is utilized as well in e-commerce widely. RSA is an asymmetric entry safety algorithm improbable DES. It is permitted algorithm. In RSA we apply two various keys, one to encryption also the rest is to decrypting. Keys are recognized like general key also confidential entry. stages of the mentioned two entries is like below:

Two expansive major data of the identical dimensions are produced; they are named p as well as q . The outcome of p plus q provides the price n . when we have condition, p also q ought to be big sufficient (the minimum 100 digits), also are preserved confidential for the delieverer. Taking into account the truth which n is the outcome of two extremely big main data, which is empirically not possible to bring out the two (i.e. p as well as q) with relative to a provided n .

An arbitrary number is subsequently chosen, called e ; in which e ought to be bigger compared to 1, also the $\text{gcd}(e, (p-1), (q-1)) = 1$ (the price of e is namedd general apparatus).

Next, discover the generative reverse of e modulo $(p-1)(q-1)$, called d (the value of d is named private exponent). The general entry is (n, e) also the confidential entry is d .

One of the big advantages of RSA algorithm is the general entry could be made also delivered to a person for example, from executive) to encrypt a letter, however merely the special entry of the allocated receiver could be applied for decrypting it [28].

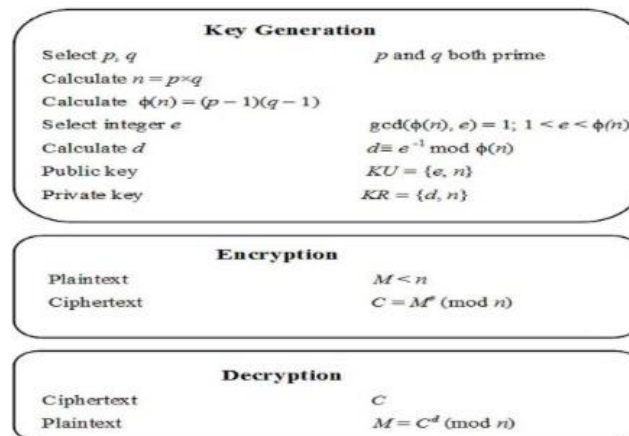


Figure 2.14. Key generation in RSA algorithm

2.10.3. Hash function

Is a direct procedure, where simple words is changed to hashed price (encrypted form). as soon as the data is confused applying a Hash Function it could not be turned again to simple words. Overall, this method is applied for password encryption, anytime we require for connecting the code accessed is encrypted applying hash function also subsequently coordinated coupled with the code saved in the database that is previously in encrypted form, when they harmonize the consumer obtains entry else it receives the letter of wrong username/password. Largest widely applied Hash Functions contains MD4, MD5, SHA, SHA-1 etc. [32]. A hash function need to align with two properties so as to be advantageous [37]:

1. The first possession has to be direct.
2. The second possession has to be clash impenetrable.

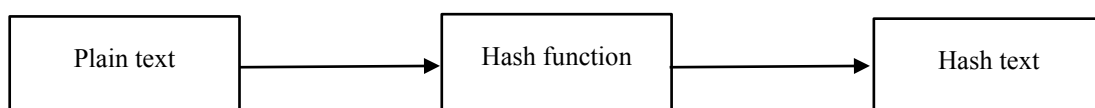


Figure 2.15. Hashing algorithm

CHAPTER 3. LITERATURE REVIEW

Authors in [10] investigated with regards to the Symmetric Encryption Algorithms performance. This study presents the evaluation of six out of the exceptional, widespread encryption algorithms: AES (Rijndael), DES, 3DES, RC2, Blowfish as well as RC6. A differentiation is implemented at different setups to per algorithm like dissimilar dimensions of data blocks, a variety of data types, battery power consumption, various key dimension as well as consequently encryption/decryption quickness. Empirical model indicates succeeding consequences.

No crucial difference is there in the exhibition of the results whether in hexadecimal base encoding alternatively in foundation 64 encoding. When modifying packet dimension, it was discovered RC6 demands fewer durations compared to the total algorithms excluding Blowfish. when it comes to modifying data category like image in position of text, it was discovered that RC2, RC6 as well as Blowfish contains drawbacks compared to other algorithms concerning spending time. Furthermore, 3DES up to now contains weak operation than algorithm DES. Lastly -when modifying key dimension (feasible just in AES and RC6 algorithms) it is shwon that bigger key dimension causes evident difference in the battery and time wasting.

The authors of [13] conducted a relative dissection of three encryption algorithms (DES, 3DES, as well as AES) based on nine criteria including, key breadth, cipher kind, block dimensions, safety, possible keys, feasible ASCII can be printed letter keys, as well as duration taken for searching the total feasible keys at 50 billion keys each moment, and so on. According to research, AES is superior to DES as well as 3DES.

Authors in [21] provide a thorough review of common symmetric key encryption algorithms for example DES, TRIPLE DES, AES, as well as Blowfish. Symmetric Key algorithms, such as RSA, are quicker than Asymmetric Key algorithms. Furthermore, Symmetric algorithms need less memory than Asymmetric encryption algorithms. Moreover, Symmetric-key encryption is more secure in comparison of Asymmetric key encryption.

Authors in [25] the AES algorithm is efficient as to quickness, duration, quantity, as well as outpouring impact.

Author in [39] discovered the capability of the algorithm depends on the key breadth. Key breadth is straight comparable for safety as well as conversely comparable for Implementation. When the key breadth is risen the safety of algorithm is as well expanded however operation decreases.

The authors in [4] examine the importance of cryptography in database security. Confidential data stored in the clear in database systems is subject to attack. No matter how many security mechanisms are implemented, there will still be certain security flaws that attackers will exploit to access the database. However, by encrypting confidential data before storing it in the archive, information leaks can be avoided. And the whole database security problem can be reduced to the protection of a few cryptographic keys.

In [36] This method is based on ASCII values. For encryption and decryption, ASCII characters are utilized with string length accompanied by numerical calculations. To crack the procedure the attacker needs much information about the plain text; a single piece of information, such as string length, is insufficient. The use of different string lengths strengthens the technique. Further operations apply and are dependent on the length of the string. Consequently, that technique does not depend on any specific key or key generation method. It is the strength of the method.

Authors in [30] suggested a symmetric encryption algorithm applying ASCII prices of figure. The presented algorithm provides positive leads to not much performing duration. The mentioned method produces key inevitably for encrypting the letter. The spontaneously produced key is changed to a distinct string as well as identical key is applied on encryption and decryption. Consequently, they identify this algorithm as symmetric key algorithm.

Authors in [14] have performed the relative dissection of three algorithms; RSA, DES as well as AES however taking account some parameters for example the length of duration, memory consumption as well as output byte. The mentioned frameworks are the primary problem to worry about in whatever Encryption Algorithm. Empirical consequences indicate DES algorithm requires minimum encryption duration as well as AES algorithm contains minimum memory application however encryption duration variety is very tiny when it comes to AES as well as DES algorithm. RSA requires largest encryption duration as well as memory utilization is as well extremely tall however output byte is minimum when it comes to RSA algorithm.

Authors in [20] are deduced that databases are the primary factor to whatever varieties of implications. Database includes extremely significant as well as private date accordingly a possibility of hacks is there. different risks on databases are explored in this study. Revision of certain significant database safety methods for example entry control, methods with relative to SQLIA, encryption as well as data deforming are explored.

The authors of [11] provide an implementation assessment of various symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish, and RC2. They discovered that when packet size is changed, Blowfish outperforms other encryption algorithms.

CHAPTER 4. METHODOLOGY

The formula was clarified using a working style chart, as seen in Figure 4.1. We used these in our formula:

1. 3 keys are created by the user and one by the programmer and the other in a variable way.
2. Two texts to create key1 and key2.
3. Ascii Code.
4. 4 Subformulas

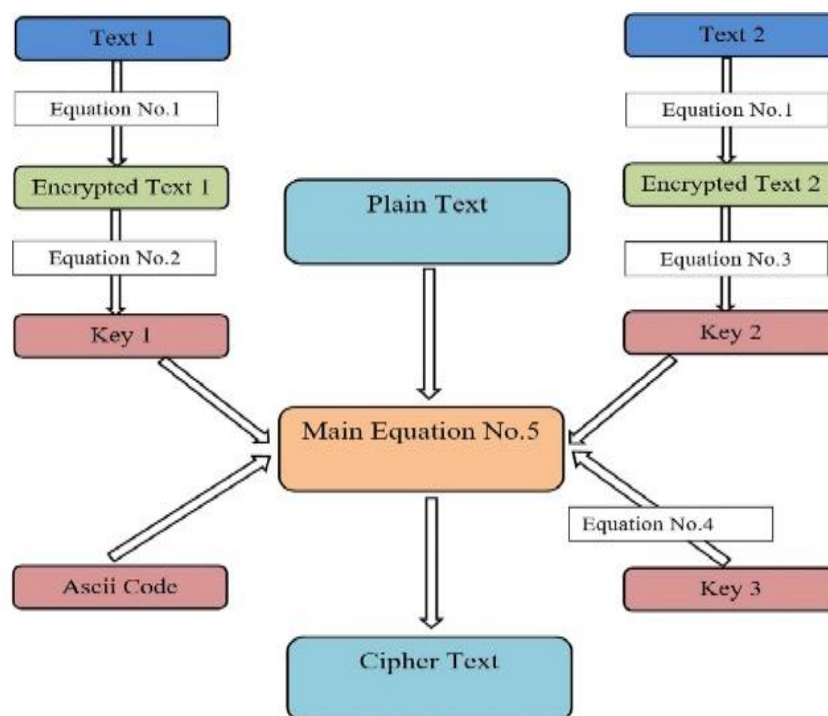


Figure 4.1. Equation diagram

In general, our formula will be applied in the following steps:

1. In the first step, we need two texts, one written by the user and the other by the programmer, the number of characters in the text should be between 8 and 50, and the character of the text is one of these characters (a-z, A-Z, 0-9, Keyboard Symbols) we'll encrypt both texts through formula number 1.

For example Text1 = Ah5\$Z2t*K7 and Text2 = @mQ4s#D7\$L

So:

Eq(1) = (Ascii code for character + sum of character number in Text)

Table 4.1. Examples of encrypting text (1) in equation (1)

Character	A	h	5	\$	Z	2	t	*	K	7
Ascii code	65	104	53	36	90	50	116	42	75	55
Eq(1)	65+10	104+10	53+10	36+10	90+10	50+10	116+10	42+10	75+10	55+10
New Ascii code	75	114	63	46	100	60	126	52	85	65
New Character	K	r	?	.	d	<	~	4	U	A

Text1 changed to Kr?.d<~4UA

Table 4.2. Examples of encrypting text (2) in equation (1)

Character	@	m	Q	4	s	#	D	7	\$	L
Ascii code	64	109	81	52	115	35	68	55	36	76
Eq(1)	64+10	109+10	81+10	52+10	115+10	35+10	68+10	55+10	36+10	76+10
New Ascii code	74	119	91	62	125	45	78	65	46	86
New Character	J	w	[>	}	-	N	A	.	V

Text2 changed to Jw[>}-NA.V

2. In the second step, we will get both Key1 and Key2 by applying two different formulas, (formula number 2 on text 1, and formula number 3 on text 2).

$$\text{Eq}(2) = ((\text{total number of all encrypted character ascii code number in Text1}) * 2) / (\text{sum of character number in Text1} - 2) = \text{Key 1}$$

Table 4.3. Key (1) generating equation

Character	K	r	?	.	d	<	~	4	U	A
Ascii code	75	114	63	46	100	60	126	52	85	65
Eq(2)	((75+114+63+46+100+60+126+52+85+65) * 2) / (10 - 2) = (786 * 2) / 8 = 196.5									

Key1 = 196 Because Key1 should be integer number

$$\text{Eq}(3) = ((\text{total number of all encrypted character ascii code number in Text2}) - \text{Key1}) / (\text{sum of character number in Text2} - 1) = \text{Key 2}$$

Table 4.4. Key (2) generating equation

Character	J	w	[>	}	-	N	A	.	V
Ascii code	74	119	91	62	125	45	78	65	46	86
Eq(2)	((74+119+91+62+125+45+78+65+46+86) - 196) / (10 - 1) = (791 - 196) / 9 = 66.11									

Key2 = 66 Because Key2 should be integer number

- In the third step, through applying a sub formula number 4, we get Key 3, which is a variable key and shifts according to the number of characters of the text we encrypt. This key plays an essential role if one character occurs in the text more than once.
- In the fourth step, we can get our encrypted letter using all three keys (1, 2, 3), with ASCII code for characters in the main formula.

We'll apply formula to this plain text (Sakarya) when know Key1 =196 and Key2 =66

$$\text{Eq}(5) = (\text{Ascii code for character} + \text{Key1}) + (\text{Key2} - \text{sum of character number in Key2}) + \text{Key3} = \text{New Ascii code.} \quad \text{For Encryption.}$$

Table 4.5. Encrypting procedure

Plain Character	Ascii code	Key1	Key2	Key3	Encryption Equation: (Ascii code + K1) + (K2 - Length of K2) + K3	New Ascii code	Cipher Character
S	83	196	66	11	$(83 + 196) + (66 - 10) + 11$	346	Š
a	97	196	66	31	$(97 + 196) + (66 - 10) + 31$	380	ž
k	107	196	66	13	$(107 + 196) + (66 - 10) + 13$	372	Ŧ
a	97	196	66	30	$(97 + 196) + (66 - 10) + 30$	379	Ž
r	114	196	66	15	$(114 + 196) + (66 - 10) + 15$	381	Ř
y	121	196	66	28	$(121 + 196) + (66 - 10) + 28$	401	Ÿ
a	97	196	66	18	$(97 + 196) + (66 - 10) + 18$	367	ů

$$\text{Eq}(5) = (\text{New Ascii code} + \text{Key1}) - (\text{Key2} - \text{sum of character number in Key2}) - \text{Key3} = \text{Ascii code} \quad \text{For Decryption}$$

Table 4.6. Decrypting procedure

Cipher Character	New Ascii code	Key1	Key2	Key3	Decryption Equation (New Ascii code + K1) - (K2 - Length of K2) - K3	Ascii code	Plain Character
Š	346	196	66	11	$(346 - 196) - (66 - 10) - 11$	83	S
ž	380	196	66	31	$(380 - 196) - (66 - 10) - 31$	97	a
Ŧ	372	196	66	13	$(372 - 196) - (66 - 10) - 13$	107	k
Ž	379	196	66	30	$(379 - 196) - (66 - 10) - 30$	97	a
Ř	381	196	66	15	$(381 - 196) - (66 - 10) - 15$	114	r
Ÿ	401	196	66	28	$(401 - 196) - (66 - 10) - 28$	121	y
ů	367	196	66	18	$(367 - 196) - (66 - 10) - 18$	97	a

If data type is number or currency then :

$$\text{Eq}(5) = (\text{value of (number or currency)} / 5) + 5 \quad \text{For Encryption}$$

For example : How to encrypt 550

$$\text{So encrypted value} = (550 / 5) + 5 = 110 + 5 = 115$$

$$\text{Eq}(5) = ((\text{Encrypted value}) - 5) * 5 \quad \text{For Decryption}$$

For example : How to decrypt 115

So decrypted value = $(115 - 5) * 5 = 110 * 5 = 550$

4.1. Practical Section

To test our formula, we designed a database from Microsoft access 2016 that consists of two parts; one to insert some data into the database table, and the other part is for testing the speed of our formula. To access our database, you must first create a user, as seen in Figure 4.2.



The image shows a 'Create User' form with a dark background. At the top, the title 'Create User' is centered. Below the title is a table with four rows and two columns. The first column contains empty input fields, and the second column contains labels: 'User ID', 'User Name', 'Password', and 'EMAIL'. Below the table are four buttons: 'delete user' (red), 'update user' (blue), 'create user' (green), and 'close form' (orange).

Figure 4.2. Create user

Then, as seen in Figure 4.3. we'll log into our database using the user and password we've developed.

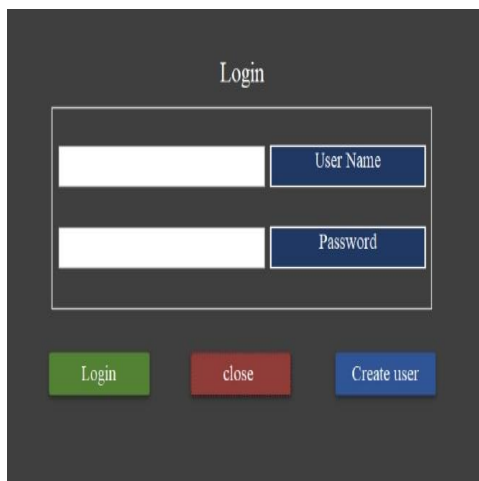


Figure 4.3. Login form

Next, we'll open a form with two sections, one of which is for data entry and the other for data recording, where Text 1 and Text 2 are used to enter information such as (Id, Full name, Age, Gender, Email) after which we'll see that the data is encrypted as seen in Figure 4.4.



Figure 4.4. Login form

In the second section, we also insert Text 1 and Text 2, and then we insert our plain text, which, after we press the encrypt command, produces ciphertext in one text box and the time to encryption in another text box. For decryption, we follow the same procedure as seen in Figure 4.5.

Text 2 by user (K ₂)	Text 1 by programmer (K ₁)	Time for encryption
wsKQp0f0117mCk0#Pzy	Sj0546&M9A4d5evRk	256ms
25733 Cipher Text Size		25733 Plain Text Size
Cipher Text	Plain Text	
gq6t0ce50jT3dHhAhtb5pZdE6P5ieG1T0u1D1LF G6b5k(Vu0ydz7qjDdND8ujZenc0n0y0pVba3p urj6a09L0baq00yFAGNp0j0j0MAG0&A0yA0d0 U5d0c0d0N0E0h0d0&0c0p0g0C0R0b0&0S0A0w0 60V0H0&0A0y0&0A0C0r0s0T0&A0U0s0B0i0c0E	95&FjP55345DdsvhytwfjTw0*ws0yoc5VAH GAScZtH#8&dZ3dhw0jsHdH23j 9r/w&PsaZG+ac2945r54rca6v@*RAN9S0FjP55 345DdsvhytwfjTw0*ws0yoc5VAHMASZtHMA 8dZ3dhw0jsHdH23Hc/w&Jfsa	
Decrypt	Encrypt	
Clear Cipher Text	Clear Plain Text	

Figure 4.5. Speed test form

CHAPTER 5. RESULT AND DISCUSSION

We will compare our algorithm to other algorithms in this section (Blowfish, DES, 3DES, RSE, and RSA). For instance, if we have data as shown in Table 5.1, we will reach the results, while you know that :

Key1 = S8r#I5h&0Da@

Key2 = t@S9&Hk4&0Fm*W

Table 5.1. Data encryption in our system

Field name	Id	Full name	Age	Gender
plain text	008821	Sivan Sper Ibrahim	33	MALE
cipher text	ļõņRŅõ	ŗŦzũŶĤSŴũŴŦnŦŦũŦŦžt	11.6	şűşű

1. When we encrypt plain text, it provides us the same size as plain text.
2. If a character appears in the text more than once, it will be encrypted with a new character each time.
3. When we encrypt text-type data, it gives us text-type data, but if we encrypt a number-type data, we get a number-type data, which is another significant point for the algorithm speed when searching for specific data.
4. Another essential point in our algorithm is that when we encrypt different characters in the plain text, the matched character will appear in the ciphertext. This is significant in terms of data security because it would be impossible to convert the encrypted character back to the original if the data is taken over by an attacker.

- Another point is the length of our Keys, which are between 8 and 50 characters, and this is a vital factor to protect our algorithm because breaking the Keys requires more time and more effort.

In order to clarify the above mentioned points in our experimental results, we gave two charts for both encrypted and decrypted texts.

The Figure 5.1. represents the original plain text which hold 52 frequencies in the same size of the text; while the Figure 5.2. represents the secured text and hold 1039 frequencies. This proves that the proposed method works well on the suggested text.

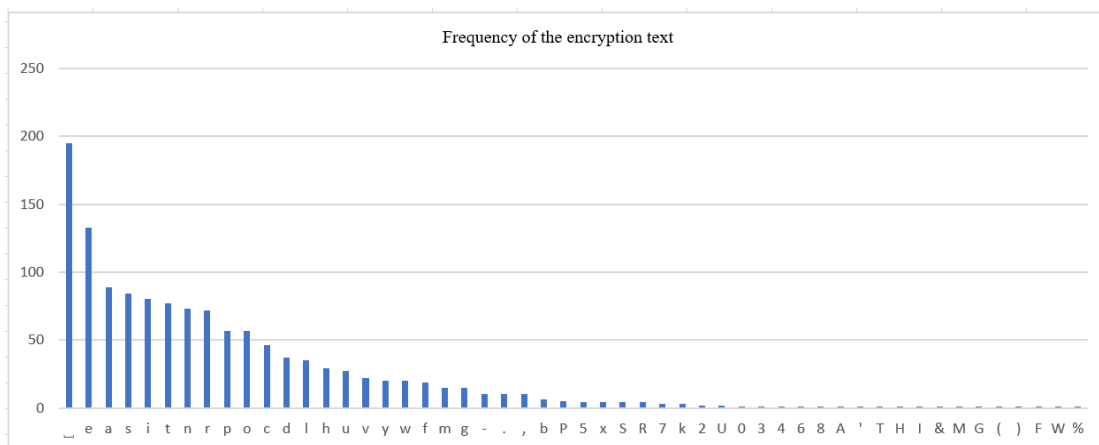


Figure 5.1. Frequency of the encryption text

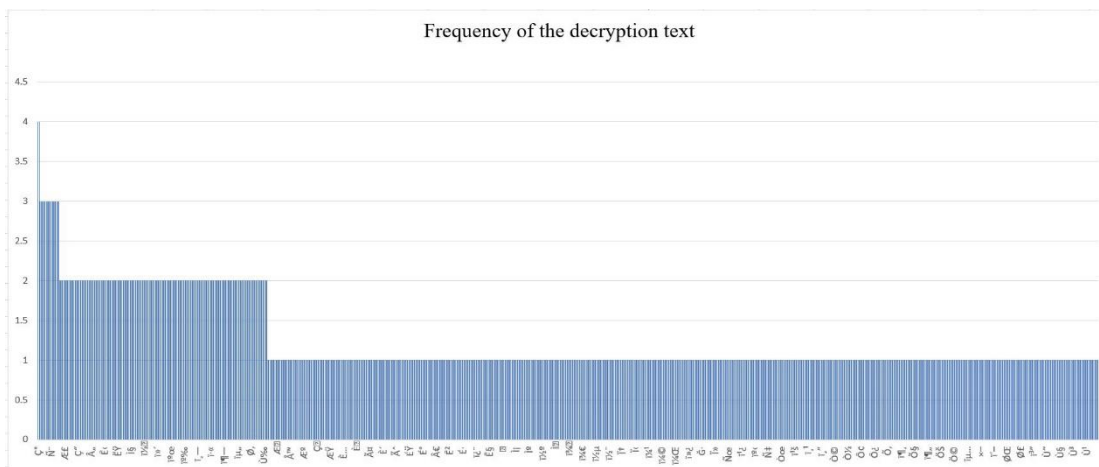


Figure 5.2. Frequency of the decryption text

To compare the speed of our algorithm, we have received the previous researches, for example, [33] here the author has got that when we encrypt 25KB file (RSA), it takes more time than other algorithms and (Blowfish) takes the least time as shown in Figure 5.3.

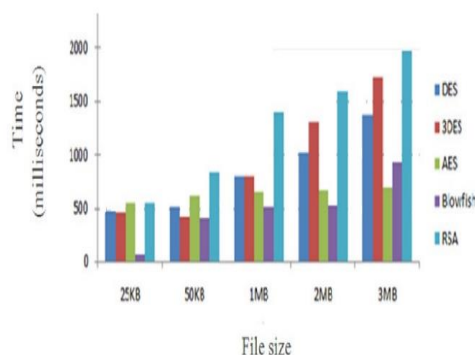


Figure 5.3. Encryption time vs. file size for DES, 3DES, AES, Blowfish, RSA

also, when we decrypt 25kb file (RSA) it takes more time than other algorithms and (Blowfish) takes the least time as shown in Figure 5.4.

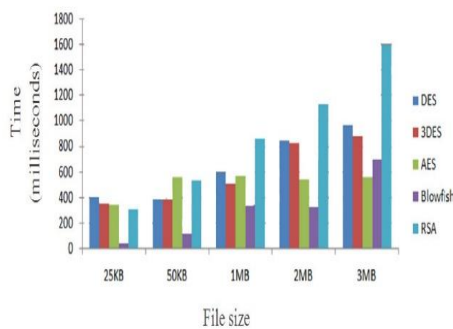


Figure 5.4. Decryption time vs. file size for DES, 3DES, AES, Blowfish, RSA

To compare a 25 KB file, we tested our method and found that we require 256ms for encryption and 272ms for decryption after five repetitions, indicating that our algorithm is quicker than all of the (RSA, DES, TDES, and RSA) in encryption as well as decryption speeds, like illustrated in Figure 5.5.

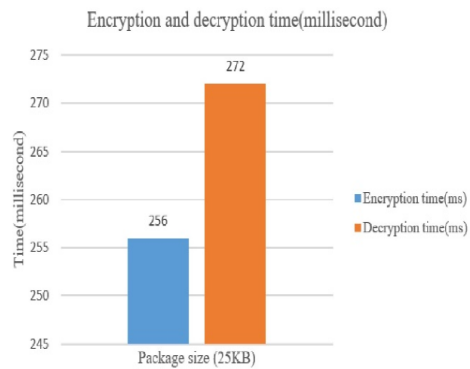


Figure 5.5. Encryption and decryption time

As a result, we will use the algorithm to create databases and encrypt data because it has large and fast data encryption security, which will secure our data from attacks.

CHAPTER 6. CONCLUSION

This thesis is a comparative study between the created logarithm for data encryption when creating databases against several different cryptographic logarithms, including (DES, 3DES, AES, Blowfish, and RSA) in terms of security and speed of encryption and decryption. The results reveal that the created logarithm is faster than the (DES, 3DES, AES, and RSA) algorithms but slower than the (Blowfish) algorithm. Also, in the created logarithm, the plain text size and the ciphertext have the same size. When we encrypt text-type data, we get text-type data. But if we encrypt a number type-data, we get a number-type data. The developed algorithm is secure. If we have more than one character in the text, each will encrypt with a different character. Also, when we encrypt various characters in plain text, the matched character will appear in the ciphertext. In future work, we can focus on the created logarithm, which we can compare with other types of cryptographic algorithms.

REFERENCES

- [1] W.Stallings, "Cryptography and Network Security", 2nd Edition, Prentice Hall, 1999.
- [2] A. Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.
- [3] Bharat B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan and K.S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167-186, 2004.
- [4] Samba Sesay, Zongkai Yang, Jingwen Chen and Du Xu, "A Secure Database Encryption Scheme" Conference Paper. February 2005 DOI: 10.1109/CCNC. 2005. 1405142. Source: IEEE Xplore.
- [5] Aamer Nadeem, Dr M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms", First International Conference on IEEE Information and Communication Technologies (ICICT), Vol 1, Issue 6, 27-28 Aug. 2005, pp 84-89.
- [6] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.
- [7] A. Nadeem, "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89, 2006.
- [8] Jason H. Li, B. Bhattacharjee, M. Yu and Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks", Journal of Future Generation Computer Systems, Elsevier Science Publishers, Vol. 24, pp. 860-869, 2008.
- [9] Hua Li and J. Li, "A New Compact Dual-Core Architecture for AES Encryption and Decryption", IEEE Canadian Journal of Electrical and Computer Engineering, Vol. 33, No. 3, pp. 209-213, 2008.

- [10] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.
- [11] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Energy Efficiency of Encryption Schemes for Wireless Devices" International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009 1793-8201.
- [12] Luc Bouganim, Yanli GUO, "Database Encryption", Article · January 2010 DOI: 10.1007/978-1-4419-5906-5_677.
- [13] Hamdan.O. Alanazi, B.B. Zaidan, A.A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal of Computing, Volume 2, ISSUE 3, March 2010, ISSN 2151-9617.
- [14] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.
- [15] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, pp. 743-754, 2012.
- [16] Basharat, I., Azam, F. and Muzaffar, A., Database Security and Encryption: A Survey Study, International Journal of Computer Applications, 47(12): 28-34 (2012).
- [17] Kulkarni, S. and Urolagin, S., Review of Attacks on Databases and Database Security Techniques, International Journal of Emerging Technology and Advanced Engineering, 2(11): 253-263 (2012).
- [18] Patil, A. and Meshram, B. B., Database Access Control Policies, International Journal of Engineering Research and Applications, 2(3): 3150–3154 (2012).
- [19] A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJCSE), Vol. 4, pp. 1650-1657, Sep 2012 ISSN: 0975- 3397.
- [20] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

- [21] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, ISSN: 0975-3397.
- [22] Rohilla, S. and Mittal, P. K., Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5): 810–813 (2013).
- [23] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.
- [24] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
- [25] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.
- [26] Kaur, R., Kiranpreet and Verma, P., Survey on Database Security, International Journal of Computer Applications, 105(10): 27–31 (2014).
- [27] Singh, S. and Rai, R. K., A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies, 5(3): 3215–3219 (2014).
- [28] Aakanksha Sharma, "Comparative Study of Symmetric Cryptography Algorithm", Faculty of Engineering, Department of Computer Science & Engineering Pacific, University (PAHER), Udaipur (Rajasthan) January 2014, En. No. PU1235.
- [29] Ms NehaKhatri – Valmik and Prof. V. K Kshirsagar "Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83.
- [30] Satyajeet R. Shinge, Rahul Patil, "An Encryption Algorithm Based on ASCII Value of Data", IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234 ISSN: 0975-9646.
- [31] Thuraisingham, B., Database Security: Past, Present, and Future, IEEE International Congress on Big Data, 772–774 (2015).
- [32] Prabhsimran Singh, Dr. Kuljit Kaur "Database Security Using Encryption", 2015 1st International conference on futuristic trend in computational analysis and knowledge management. DOI: 10.1109/ABLAZE.2015.7155019.

- [33] Priyadarshini Patil, Prashant Narayana ,Narayan D G, Meena S M, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish” International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.
- [34] Manchikatla, Swarna Rekha, "Design of a Data Encryption Test-Bed Used to Analyze Encryption Processing Overhead" (2016). Culminating Projects in Information Assurance. 12.
- [35] Emad F. Khalaf and Mustafa M. Kadi., “A Survey of Access Control and Data Encryption for Database Security”, JKAU: Eng. Sci., Vol. 28 No. 1, pp: 19 - 30 (1438 A.H./ 2017 A.D.) Doi: 10.4197/Eng. 28-1.2.
- [36] Er. Suraj Arya, Dr.Ankit Kumar, “ASCII BASED ENCRYPTION DECRYPTION TECHNIQUE FOR INFORMATION SECURITY AND COMMUNICATION,” Conf.YMCA, Connaught Place, New Delhi 7th January 2017,ISBN:978-93-86171-27-6.
- [37] Abdalbasit Mohammed Qadir, Nurhayat Varol, “A Review Paper on Cryptography”, Conference Paper · June 2019, DOI: 10.1109/ISDFS.2019.8757514.
- [38] Uma Pujeri, Ramachandra Pujeri, “Symmetric Encryption Algorithm using ASCII Values”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-5, January 2020.
- [39] Hitesh Mittal, “Optimized Encryption Algorithm using Dynamic Keys”, Electronics and Communication Engineering Department, THAPAR UNIVERSITY PATIALA-147004, Roll. No. 801261010.
- [40] www.edureka.co/blog/what-is-a-database/, Access Date: 10/5/2021
- [41] www.sumologic.com/blog/what-is-database-security/, Access Date: 10/5/2020

RESUME

Name and Surname: Sivan Sper IBRAHIM

EDUCATION STATUS

Degree	Education Unit	Graduation Year
MSc	T.C. Sakarya University/Department of Computer and Information Engineering	Ongoing
Undergraduate	Sulaymaniyah university/College of Commerce/Statistic and Computer	2011
High School	Sulaymaniyah, Iraq	2007

WORK EXPERIENCE

Year	Location	Task
2020-Present	Sakarya University	Master Student
2011-Present	Sulaymaniyah university	Researcher

FOREIGN LANGUAGE

English, Arabic, Turkish

HOBBIES

Reading, Writing, Physical Exercises (Fitness and Football)