ENCRYPTION IN CRYPTOGRAPHY

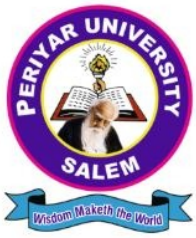
Dissertation submitted to Periyar University in partial fulfillment of the requirements for the award of the degree of

MASTER OF SCIENCE
IN
MATHEMATICS

Submitted by

TAMILSELVAN N
Reg. No: U22PG518MAT036

Under the guidance of
Dr. M. SAMBATH
Assistant Professor



Department of Mathematics
Periyar University
Periyar Palkalai Nagar
Salem 636 011

April 2024

CERTIFICATE

This is to certify that the dissertation entitled **" ENCRYPTION IN CRYPTOGRAPHY "** submitted in partial fulfillment of the requirements for the award of the degree of **Master of Science in Mathematics** to the Periyar University, Salem is a bonafide record of the dissertation work carried out by **TAMILSELVAN N (Reg. No: U22PG518MAT036)** under my supervision and guidance in the academic year 2023-2024 and that no part of the dissertation has been submitted for the award of any degree, diploma, fellowship or other similar titles to any university.

Date : **Signature of the Guide**

Place :

Signature of the
Head of the Department **External Examiner**

DECLARATION

I, **TAMILSELVAN N,** hereby declare that the dissertation, entitled**"ENCRYPTION IN CRYPTOGRAPHY"** submitted to the Periyar University, Salem in partial fulfillment of the requirements for the award of the degree of **Master of Science in Mathematics**, is a bonafide record of the dissertation work done by me during 2023-2024 under the guidance of **Dr.M. SAMBATH**, Assistant Professor, Department of Mathematics, Periyar University, Salem.

Date : **Signature of the Candidate**

Place : (**TAMILSELVAN N**)

ACKNOWLEDGEMENT

I express my deep sense of gratitude and indebtedness to my guide, **Dr. M. Sambath**, Assistant Professor, Department of Mathematics, Periyar University, Salem, who has been a steady source of motivation and help throughout. I am really grateful to her for her invaluable guidance, encouragement and suggestions at each and every stage of this dissertation.

I wish to acknowledge my sincere thanks to **Dr.C. Selvaraj**, Professor and Head (Retired); **Dr.A. Muthusamy**, Professor and Head; **Dr.P. Prakash**, Professor; **Dr.M. Muthulakshmi**, Professor; **Dr.S. Karthikeyan**, Assistant Professor; **Dr.S. Padmasekaran**, Assistant Professor; Non-teaching staffs and Research scholars of Department of Mathematics, Periyar University, Salem.

I also express my thanks to my **friends and well-wishers** for their full cooperation and help. I would like to express heartful thanks to my family members for their encouragement and constant help.

(***TAMILSELVAN N***)

Contents

1 Introduction **1**

2 Preliminaries **5**

3 Encryption **10**

3.1 Cryptosystems 14

3.2 Types of Symmetric Encryptions 15

3.2.1 Data Encryption Standard 16

3.2.2 Adavnced Encryption Standard 17

3.2.3 Triple Data Encryption Standard 17

3.3 Types of Asymmetric Encryptions 18

3.3.1 RSA Algorithm 18

3.3.2 Eliptic Curve Cryptography 20

3.3.3 ElGamal Algorithm 21

3.4 Types of attacks 23

4 Applications **28**

4.1 Applications Of Encryption: 28

4.2 Disadvantages: 31

5 Conclusion **32**

Chapter 1

Introduction

The word encryption derives from the Greek word kryptos, which means hidden. It is a way to store and share information privately so that only the intended recipient can understand its meaning. Encryption is based on cryptography, the process of creating and using ciphers. People have been enciphering written information for nearly 4,000 years, though ciphers became more sophisticated just over 2,000 years ago in ancient Greece.

In this modern era Cryptography really matured as a field of study with the advent of computer technology. Instead of relying on complex mechanical devices, computers could use mathematical equations and algorithms to create better encryption. The two common algorithms used today are the Symmetric Key Algorithm and the Public Key Algorithm.

Through the early 1970s, cryptology was dominated by governments both because computers were very expensive and because of the need for information retention. Several factors pushed encryption towards the mainstream. The most important of these was the invention of the World Wide Web in 1989 and the widespread use

of computers. Both industrial-commercial and personal communication had to be protected. For example, financial services were some of the first to require secure electronic transactions. Other businesses wanted to secure their digitally stored trade secrets. Finally, individuals wanted to rest assured that their online communication was secure.

Today virtually all digital communication is encrypted. It is now clear that cloud computing is the way forward for a flower, also known as a bloom or blossom, is the reproductive structure found in flowering plants (plants of the division angiospermae). Flowers consist of a combination of vegetative organs–sepals that enclose and protect the developing flower, petals that attract pollinators, and reproductive organs that produce gametophytes, which in flowering plants produce gametes. The male gametophytes, which produce sperm, are enclosed within pollen grains produced in the anthers. The female gametophytes are contained within the ovules produced in the carpels.

Most flowering plants depend on animals, such as bees, moths, and butterflies, to transfer their pollen between different flowers, and have evolved to attract these pollinators by various strategies, including brightly colored, conspicuous petals, attractive scents, and the production of nectar, a food source for pollinators. In this way, many flowering plants have co-evolved with pollinators to be mutually dependent on services they provcontentide to one another in the plant's case, a means of reproduction; in the pollinator's case, a source of food.

When pollen from the anther of a flower is deposited on the stigma, this is called pollination. Some flowers may self-pollinate, produc-

ing seed using pollen from a different flower of the same plant, but others have mechanisms to prevent self-pollination and rely on cross-pollination, when pollen is transferred from the anther of one flower to the stigma of another flower on a different individual of the same species. Self-pollination happens in flowers where the stamen and carpel mature at the same time, and are positioned so that the pollen can land on the flower's stigma. This pollination does not require an investment from the plant to provide nectar and pollen as food for pollinators. Some flowers produce diaspores without fertilization (parthenocarpy). After fertilization, the ovary of the flower develops into fruit containing seeds.

Flowers have long been appreciated by humans for their beauty and pleasant scents, and also hold cultural significance as religious, ritual, or symbolic objects, or sources of medicine and food. Nearly all users, including enterprises. Nevertheless, the question of how data security, privacy, and integrity can be reinforced remains. Companies increasingly understand the importance of confidentiality (see GDPR, ePrivacy Regulations) and demand transparency, alongside proper security controls from cloud providers. The future of encryption and decryption will have to address how data is handled by cloud services and their customers. Quantum-safe cryptography methods are in development. For example, lattice cryptography would ensure that data is hidden by embedding it inside complex math problems (or algebraic structures) called lattices.

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus

preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Chapter 2

Preliminaries

Definition 2.1. *An encryption scheme or cryptosystem is a tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *with the following properties:*

1. $\mathcal{P}$ *is a set. It is called the plaintext space. Its elements are called plaintexts.*

2. $\mathcal{C}$ *is a set. It is called the ciphertext space. Its elements are called ciphertexts.*

3. $\mathcal{K}$ *is a set. It is called the key space. Its elements are called keys.*

4. $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$ *is a family of functions* $E_k : \mathcal{P} \to \mathcal{C}$. *Its elements are called encryption functions.*

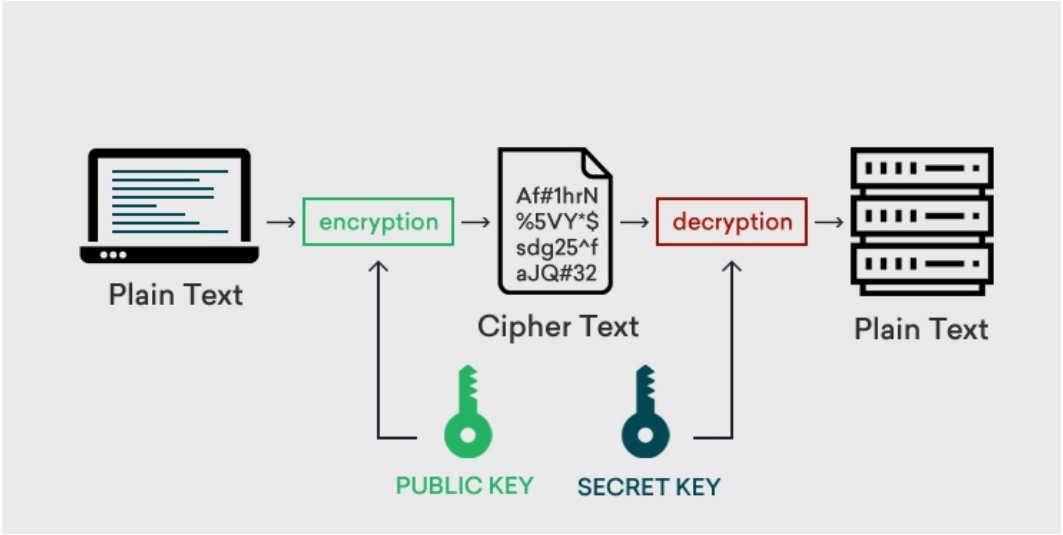
5. $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ *is a family of functions* $D_k : \mathcal{C} \to \mathcal{P}$. *Its elements are called decryption functions.*

6. *For each* $e \in \mathcal{K}$*there is a* $d \in \mathcal{K}$ *such that* $D_k(E_e(p))$=p *for all* $p_1, \mathcal{P}$,

where

- Plaintext is usually ordinary readable text before it is encrypted into ciphertext (or) readable text after it is decrypted.

- Ciphertext is encrypted text transformed form plaintext using an encryption algporithm. Ciphertext cann't be read until it has been converted in to plaintext with a key.
- A keyspace is the the set of all valid possible distinct keys of a given cryptosystem. Cryptosystems have a natural limit to the number of keys by nature of the rules in place.
- The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.
- Encryption is the method by which information is converted into secret code yhat hides the information's true meaning.



Alice can use an encryption scheme to send a confidential message m to Bob. She use an encryption key e. Bob uses the corresponding decryption key d. Alice computes the ciphertext $c = E_e(m)$ and send it to Bob. Bob can then obtain the plaintext as $m = D_d(c)$. Clearly, the decryption key must be secret.

Definition 2.2. *(Caesar cipher) The plaintext space, ciphertext space, and key space are* $\sum = \{A, B, ..., Z\}$. *We identify the letters A,B,...,Z*

according to the number $0, 1, ..., 25$. *This enables us to compute with letters. For* $e \in \mathbb{Z}_{26}$, *the encryption function* E_e *is*

$$E_e : \sum \to \sum, x \mapsto (x + e) \, mod \, 26.$$

Analogously, for $d \in \mathbb{Z}_{26}$ *the decryption function* D_d *is*

$$D_d : \sum \to \sum, x \mapsto (x - d) \, mod \, 26.$$

The decryption function key for the encryption key e *is* $d = e$. *This is, however, not true for every cryptosystem.*

The Caesar cipher can easily be modified such that the plaintext space and the ciphertext space are the set of all sequences $w = (w_1, w_2, ..., w_n)$ *with* $w_i \in \sum, 1 \leq i \leq n$. *Again, the key space is* $\mathbb{Z}_{26}$. *The encryption function* E_6 *replaces each letter* w_i *by* $w_i + e \; mod \; 26, 1 \leq i \leq n$. *This also is called the Ceaser cipher.*

Definition 2.3. *To increase the secrity of a block cipher, it is possible to apply it a few times. Frequently, the E-D-E triple encryption is used. A plaintext* p *is encrypted as*

$$c = E_{k_1}(D_{k_2}(E_{k_3}(p))).$$

Here, $k_i, 1 \leq i \leq 3$ *are three keys,*D_{k_i} *is the decryption function for key* $k_i, 1 \leq i \leq 3$. *This result in a considerably larger key space. If we only want to double the key length, we use* $k_1 = k_3$.

Definition 2.4. *To write texts, we we need symbols from alphabet. By an alphabet we mean a finite nonempty set* $\sum$. *The length of* $\sum$ *is the number of elements in* $\sum$. *The elements of* $\sum$*are called symbols or letters.*

Example 2.1. *A common alphabet is*
$\sum = \{A, B, C, D, E, F, G, H, I, J, K, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$
It has length 26.

Definition 2.5. *Let* $\sum$ *be an alphabet.*

1. *A word or string over* $\sum$ *is a finite sequence of symbols from* $\sum$ *including the empty sequence, which is denoted by* ϵ *and is called the empty string.*

2. *The length of a word* $\boldsymbol{w}$ *over* $\sum$ *is the number of its components. It is denoted by* $\mid \boldsymbol{w} \mid$ *. The empty word has length 0.*

3. *The set of all words over* $\sum$ *including the empty string is denoted by* $\sum^*$ *.*

4. *If* $\boldsymbol{v}, \boldsymbol{w} \in \sum^*$*, then* $\boldsymbol{vw} = \boldsymbol{v} \circ \boldsymbol{w}$ *is the string that is obtained by contacting* $\boldsymbol{v}$ *and* $\boldsymbol{w}$*. It is called the concatation of* $\boldsymbol{v}$ *and* $\boldsymbol{w}$*. In particular, we have* $\boldsymbol{v} \circ \epsilon = \epsilon \circ \boldsymbol{v} = \boldsymbol{v}$*.*

5. *If* n *is a nonnegative integer, then* $\sum^n$ *is the set of all words of length* n *over* $\sum$*.*

   It is shown that $(\sum^*, \epsilon)$ *is a monoid whose netural element is the empty word.*

Example 2.2. *A word over the alphabet COCA has length four. Another word over* $\sum$ *is COLA. The concentration of COCA and COLA is COCACOLA.*

Definition 2.6. *Let* X *be a set. A permutation of* X *is bijective map* $f : X \to X$*. The set of all permutations of* x *is denoted by S(X).*

Definition 2.7. *The cryptosystem has perfect secrecy if the events that a particular plaintext has been encrypted are independent (i.e.,* $Pr(p|c) = Pr(p)$*) for all plaintexts* p *and all ciphers* c*.)*

Definition 2.8. *Let S be a set containing n distinct objects. A permutation of S is an ordered list of the objects in S. A permutation of the set $\{1,2,\ldots,n\}$ is simply called a permutation of n.*

Remark 2.1. *(Fermat's Little Theorem)*
Let p be a prime number and let a be any integer. Then

$$a^{p-1} = \begin{cases} 1\,(mod\,p) & if\ p \nmid a, \\ 0\,(mod\,p) & if\ p \mid a. \end{cases}$$

Definition 2.9. *The cryptosystem of this section has perfect secrecy if the events that a particular ciphertext occurs and that a particular plaintext has been encrypted are independent (i.e., Pr(p|c) = Pr(p) for all plaintext p and all ciphertext c).*

Chapter 3

Encryption

Theorem 3.1. *The encryption functions of a block ciphers are permutations.*

Proof. Since for each encryption function there is a corresponding decryption function, the encryption functins are injective. An injective map $\sum^n \to \sum^n$ is bijective.
The most general block cipher can be described as follows. Fix the block length n and an alphabet $\sum^n$. As plaintext space and ciphertext space use $\mathcal{P} = \mathcal{C} = \sum^n$. The key space is the set $\mathrm{S}(\sum^n)$ of all permutations of $\sum^n$. The encryption function for a key $\pi \in \mathrm{S}(\sum^n)$ is

$$E_\pi : \sum^n \to \sum^n, \mathrm{v} \longmapsto \pi(v).$$

The corresponding decryption function is

$$D_\pi : \sum^n \to \sum^n, \mathrm{v} \longmapsto \pi^{-1}(v).$$

The key space of this scheme is very large. It contains $(\mid \sum \mid^n)!$ elements. Therefore, the scheme seems quite secure. It is, however rather inefficient since it is not clear how to represent and evaluate an arbitrary $\pi \in (\mid \sum \mid^n)XS$ efficiently. Therfore, it makes sense to use as the key space only a subset of all possible permutations of

$|\sum|^n$. Those permutations should be easy to present and evaluate.

It is, for example, possible to use the permutation cipher. It uses only permutations that permute the positions of the symbol. If $\sum = 0, 1$ then those are the bit permutations. The key space is the permutation group S_n. For $\pi \in S_n$, set
$E_\pi : \sum^n \to \sum^n, (v_1, v_2, ..., v_n) \mapsto (v_\pi(1), v_\pi(2), ..., v_\pi(n))$.
The corresponding decryption function is
$D_\pi : \sum^n \to \sum^n, (x_1, x_2, ..., x_n) \mapsto (x_{\pi^{-1}}(1), x_{\pi^{-1}}(2), ..., x_{\pi^{-1}}(n))$.
The key space of the permutation cipher has $n!$ elements. Each key can be encoded as a sequence of n integers $\{0, 1, ..., n-1\}$. □

A method to study the security of block ciphers consists in studying their algebirc properties. Each encryption function is an element of a permutation group. If its order is small, the decryption can be iterating the encryption function a few times.

Example 3.1. *A permutatin cipher is block cipher that works on* $\mathcal{P} = \mathcal{C} \sum^n$ *for some* $n \in \mathbb{N}$ *and uses* $\mathcal{K}' = \mathcal{K} = S_n$. *In this way* $|\mathcal{K}'| = n!$ *which is much samller than* $|S(\sum^n)|$. *Let* $\pi \in \mathcal{K}$:

$$\mathcal{E}_\pi : \sum^n \to \sum^n, (v_1, ..., v_n) \mapsto (v_{\pi(1)}, ...v_{\pi(n)}),$$

$$\mathcal{D}_\pi : \sum^n \to \sum^n, (v_1, ..., v_n) \mapsto (v_{\pi^{-1}(1)}, ...v_{\pi^{-1}(n)}).$$

For example, let $n = 3$ *and* $\sum = \mathbb{Z}/2\mathbb{Z}$. *We use the keyspaces*

$$\mathcal{K}' = \mathcal{K} = S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

with 3! *elements. Now we could, for example, encrypt the plaintext* $(v_1, v_2, v_3) = (1, 0, 1) \in \sum^3$ *via* $\pi = (123)$: $\mathcal{E}_\pi((1, 0, 1)) = (v_2, v_3, v_1) = (0, 1, 1)$.

Theorem 3.2. *The group S_n has order $n! = 1 * 2 * ... * n$.*

Proof. We prove this assertion by induction on n. Cleraly, S_1 has order 1. Suppose $S_n - 1$ has order $(n-1)!$. Consider the permutations of the set { 1,2,...,n}. We count the number of permutaton s that send 1 to a fixed number x. In such permutations, the numbers $2, ..., n$ are bijectively mapped to the numbers $1, 2, ..., x-1, x+1, ..., n$. By induction hypothesis, there are $(n-1)!$ such bijections. But since there are n possibilities to map 1 to a number, the orderb of S_n is $n(n-1)! = n!$.

Let $X = \{0,1\}_n$ be the set of all bistrings of length n. A permutation of X in which just the positions of the bits are permuted is called a bit *permutation*. To formally describe such a bit permutation, we choose $\pi \in S_n$. Then

$$f : \{0,1\}^n \to \{0,1\}^n,\ b_1...b_n \mapsto b_{\pi(1)}...b_{\pi(n)}$$

is in fact a bit permutation, and every bit permutation can be uniquely written in this way. Therefore, there are $n!$ bit permutations of bitstrings of length n.

special bit permutations are circular left or right-shifts. A circular left-shift of i positions maps the bitstring $(b_0, b_1, ..., b_{n-1})$ to $(b_{imodn}, b_{(i+1)modn}, ..., b_{(i+n-1)modn})$. Circular right-shifts are defined analogously. □

Theorem 3.3. *Let $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}| < \infty$ and Pr(p) > 0 for any plaintext p. Our cryptosystem has perfect secrecy if and only if the probability distribution on the key space is the uniform distribution and if for any plaintext p and any ciphertext c there is exactly one key k with $E_k(p) = c$.*

Proof. Suppose that the cryptosystem has perfect secrecy. Let p be

a plaintext. If there is a ciphertext c for which there is no key k with $E(p) = C$, then $\Pr(p) \neq \Pr(p|c) = 0$ since $\Pr(p) >$ by assumption. This contradicts the perfect secrecy. Hence, for any ciphertext c there is a key k with $E_k(p) = c$. But the number of keys is equal to the number of cipherexts. Therefore, for each ciphertext c there is exactly one key k with $E_k(p) = c$. T is proves the second assertion.

To prove the first assertion, we fix a ciphertext c. For a plaintext p, let $k(p)$ be the uniquely determined key with $E_{k(p)}(p) = c$. Then we have

$$\mathcal{K} = \{k(p) : p \in \mathcal{P}\} \tag{3.1}$$

since the number of plaintext is equal to the number of keys. Below we show that all $p \in \mathcal{P}$ the probability of $k(p)$ is equal to the probability of c. Then the probability of $k(p)$ does not depend on p. Hence the probability of all $k(p)$ is the same. Since by (3.1) every key $k \in \mathcal{K}$ is equal to $k(p)$ for some $p \in \mathcal{P}$, the probability distribution the key space is the uniform distribution.

Let $p \in \mathcal{P}$. As promised, we show that $\Pr(k(p)) = \Pr(c)$. Then

$$Pr(p|c) = \frac{Pr(c|p)Pr(p)}{Pr(c)} = \frac{Pr(k(p))Pr(p)}{Pr(c)}. \tag{3.2}$$

Since the cryptosystem has perfect secerecy, we have $\Pr(p|c) = \Pr(p)$. So (3.2) implies $Pr(k(p)) = Pr(c)$, as asserted.

Now we prove the converse. Assume that the probability distribution on the key space is the uniform distribution and that for any plaintext p and any ciphertext c there is exactly one key $k = k(p, c)$ with $E_k(p) = c$. Then

$$Pr(p|c) = \frac{Pr(p)Pr(c|p)}{Pr(c)} = \frac{Pr(p)Pr(k(p,c))}{\sum_{q\in\mathcal{P}} Pr(q)Pr(k(q,c))}. \tag{3.3}$$

Now $\Pr(k(q,c)) = 2/|\mathcal{K}|$ for all $q \in \mathcal{P}, c \in \mathcal{C}$. Since all keys are equallay probable. Hence,

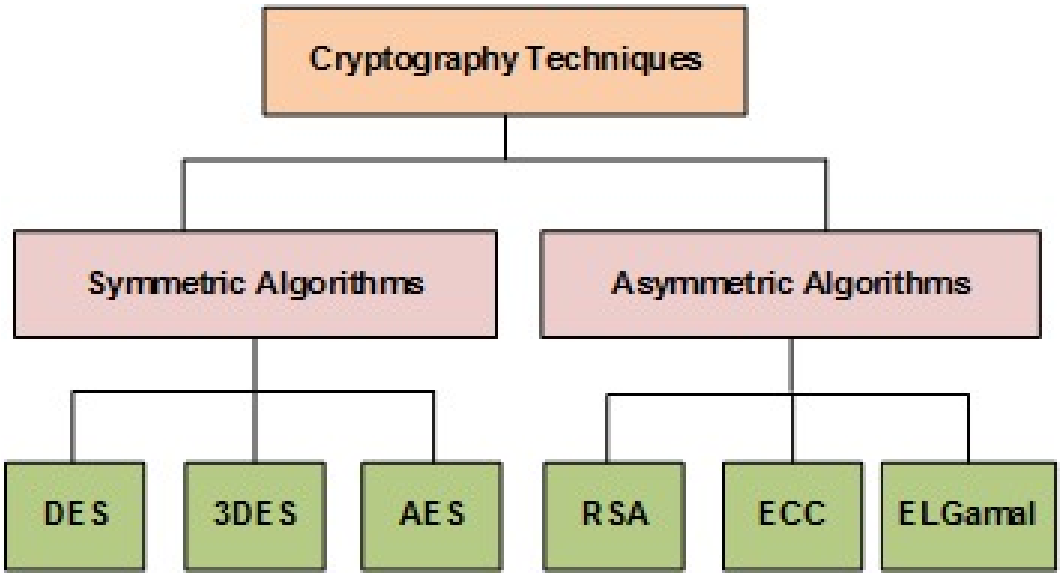
$$\sum_{q\in\mathcal{P}} Pr(q)Pr(k(q,c)) = \frac{\sum_{q\in\mathcal{P}} Pr(q)}{|\mathcal{K}|} = \frac{1}{|\mathcal{K}|}$$

If we use this equation in (3.3), then we obtain $\Pr(p|c) = \Pr(p)$, as asserted. □

3.1 Cryptosystems

The two types of data encryption are symmetric and asymmetric encryption.

1. Symmetric encryption
2. Asymmetric encryption



If Alice wants to send an encrypted message to Bob, then she uses an encryption key and Bob uses the corresponding decryption key to recover the plaintext.

If in a cryptosystem the encryption key e is alwaysequal to the decryption key d, or if d can be easily computed from e, then the

cryptosystem is called *symmetric.* It focuses on a similar key for encryption as well as decryption. Most importantly, the symmetric key encryption method is also applicable to secure website connections or encryption of data. It is also referred to as secret-key cryptography. The only problem is that the sender and receiver exchange keys in a secure manner. The popular symmetric- key cryptography system is Data Encryption System(DES). The cryptographic algorithm utilizes the key in a cipher to encrypt the data and the data must be accessed. A person entrusted with the secret key can decrypt the data. Examples: AES, DES, etc.

In asymmetric cryptosystems, the key d and e are distinct, and the computation of d from e is infeasible. In such systems, the encryption key can be made public.his cryptographic method uses different keys for the encryption and decryption process. This encryption method uses public and private key methods. This public key method help completely unknown parties to share information between them like email id. private key helps to decrypt the messages and it also helps in the verification of the digital signature. The mathematical relation between the keys is that the private key cannot be derived from the public key, but the public key can be derived from the private key. Example: ECC,DSS etc.

3.2 Types of Symmetric Encryptions

Symmetric cryptography is placed in the category of cryptography schemes in which a shared key is used to convert a plaintext into cipher text. A same secret key is shared by both sender and receiver.

Followings are the symmetric cryptography schemes.

1. Data Encryption Standard
2. Adavnced Encryption Standard
3. Triple Data Encryption Standard

3.2.1 Data Encryption Standard

A block of ciphertext consists of 64 bits. Thekey has 56 bits, but is expressed as a 64 bit string. The 8th, 16th, 25th,..., bits are parity bits, arranged so that each block of 8 bits has an odd number of 1s. This is for error detection purposes. The output of the encryption is 64 bit ciphertext. The bits of m are permuted by a fixed initial permutation to obtain $m_0IP(m)$. Write $m_0L_0R_0$, where L_0 is the first 32 bits of m_0 and R_0 is the last 32 bits.
The DES algorithm, starts with a planintext m of 64 bits, and consists of three stages:

1. The bits of m are permuted by a fixed initial permutation to obtain. $m_0 = IP(m)$. Write $m_0 = L_0R_0$, where L_0 is the first 32 bits of m_0 and R_0 is the last 32 bits.

2. For $1 \leq i \leq 16$, perform the following:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

   where k_i is a string of 48 bits obtained from the key K and f is a function to be described later.

3. Switch left and right to obtain $R_{16}L_{16}$, then apply the inverse of the initial permutation to get the ciphertext $c = IP^{-1}(R_{16}L_{16})$. The DES algorithm is a so called $Feistelcipher$

3.2.2 Adavnced Encryption Standard

The Advanced Encryption Standard (AES) algorithm as the industry standard. Despite being quite effective in 128-bit version, AES also employs keys of 192 and 256 bits for use in heavy-duty encryption. With the exception of brute force, which tries to read communications by utilizing every combination of the 128, 192, or 256-bit cipher, AES is generally thought to be immune to all assaults. AES is a block cipher with alphabet $\mathbb{Z}_2$. It is a special case of the Rijndeal cipher.

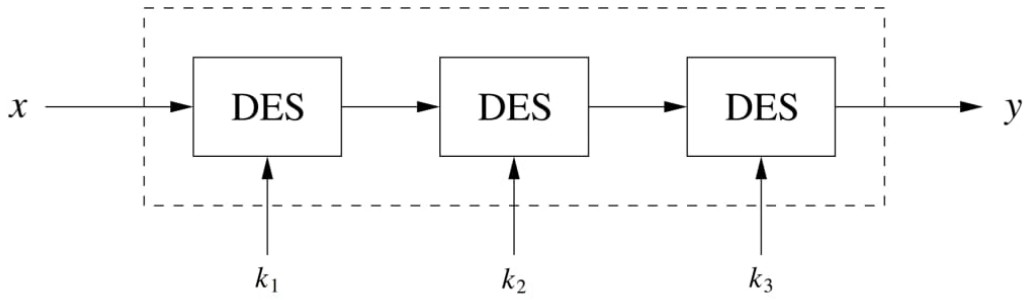
Morden symmetric ciphers such as the *DataEncryptionStandard* (DES) and the *AdvancedEncryptionStandard* (AES) are based on ad hoc mixing operations, rather on intractable mathematical problems used by asymmetric ciphers. The reason that DES and AES and other symmetric ciphers are used in practice is that they are much faster than asymmetric ciphers. Thus if Alice wants to send Bob a long message, she first uses an asymmetric cipher such as RSA to send Bob a key for a symmetric cipher, and then she uses a symmetric cipher such as DES or AES to send the actual data.

3.2.3 Triple Data Encryption Standard

An alternative to AES or the AES finalist algorithms is triple DES, often denoted as 3DES. DES consists of three subsequent DES encryptions

$$y = DES_{k3}(DES_{k2}(DES_{k1}(x)))$$

with different keys, as shown as



3.3 Types of Asymmetric Encryptions

Asymmetric cryptography is also in the category of cryptography schemes. Unlike symmetric cryptography, two keys are used: one is public and second is private. The public key is shared by anyone in the cryptographic system while the private key is kept secret by authenticated user. Followings are the asymmetric cryptography algorithms.

1. RSA Algorithm
2. Eliptic Curve Cryptography
3. ElGamal

3.3.1 RSA Algorithm

The industry standard for encrypting data exchanged over the internet is the public-key algorithm RSA. It also happens to be a technique employed by PGP and GPG software. Due to the usage of a pair of keys, RSA is regarded as an asymmetric algorithm as opposed to triple DES.
The security of RSA depends on the on the following dichotomy:

- **Setup.** Let p and q be large primes, $letN = pq$, and let e and c be integers.
- **Problem.** Slove the congruence $x^e = c(modN)$ for the variable x.
- **Easy.** Bob, who knows the values of p and q, cannot easily find x. as described.
- **Hard.** Eve, who does not not know the values of p and q, cannot easily find x.
- **Dichotomy.** Sloving $x^e \equiv c\,(modN)$ is easy for a person who possesses certain extra information, bt it is apparently hard for all other people.

Example 3.2. *Bob's RSA public key has modulus N = 12191 and exponent e = 37. Alice sends Bob the ciphertext c = 587. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. (Hint. N has a factor smaller than 100.)*

Solution

The modulus factors as N = 12191 = 73·167, so $\phi(N) = 72{\cdot}168 = 11952$.

The congruence

$$37d \equiv 1\,(mod\,11952)$$

has solution $d \equiv 11629\,(mod\,11952)$. Then

$$m \equiv 587^{11629} \equiv 4894\,(mod\,12191)$$

is a solution to $m^{37} \equiv (mod\,12191)$.

It is posible to be a bit more efficient, using the fact that

g= gcd(72,166) = 2 and (72)(166)/ = 5976. Thus a solution to the congruence

$$37d \equiv 1\,(mod\,5976)$$

is a decryption exponent $d \equiv 5653(mod\,5976)$. Of course, this gives the same plaintext

$$m \equiv 587^{5653} \equiv 4894(mod\,12191).$$

3.3.2 Eliptic Curve Cryptography

Elliptic curves can be defined over any fiel. In cryptography, elliptic curves over finite fields are of particular interest. To make things simple, we only describre elliptic curves over prime fields.
Let p be a prime number, $p > 3$ and let $a, b \in GF(p)$. consider the equation

$$y^2z = x^3 + axz^2 + bz^3. \tag{3.4}$$

Its discriminant is

$$\Delta = -16(4a^3 + 27b^2). \tag{3.5}$$

We assume that Δ is nonzero. If $(x, y, z) \in GF(p)^3$ is a solution of this eauation, then for any $c \in GF(p)$ also $c(x, y, z)$ is a solution. Two solutions (x,y,z) and (x',y',z') are called equivalent if there is a nonzero $c \in GF(p)$ with (x,y,z) = c(x',y',z'). This defines an equivalence relation on the set of all solutions of (3.4). The equivalence class of (x,y,z) is denoted by (x : y : z). The $elliptic\,curve E(p; a, b)$ is the set of all equivalence classes of solutions of (3.4). Each element of this set is called a point on the curve. ECC is a modern encryption algorithm that provides greater security with shorter key lengths.

3.3.3 ElGamal Algorithm

Alice wants to send a message m to Bob. Bob choose a large prime p and a primitive root α. Assume m is an integer with $0 \leq m < p$. If m is larger, break it into smaller blocks. Bob also chooses a secret integer a and computes $\beta \equiv \alpha^a \pmod{p}$. The information (p, α, β) is made public and is Bob's public key. Alice does the following:

1. Downloads (p, α, β).
2. Choose a secert random integer k and computes $r \equiv \alpha^k \pmod{p}$.
3. Computes $t \equiv \beta^m \pmod{p}$.
4. Sends the pair (r, t) to Bob.

Bob decrypts by computing

$$tr^{-a} \equiv m(mod\, p)$$

This works because

$$tr^{-a} \equiv \beta^k m(\alpha^k)^{-a} \equiv (\alpha^a)^k m\alpha{-}ak \equiv m(mod\, p).$$

Example 3.3. *Alice and Bob agree to the prime $p = 1373$ and the base $g = 2$ for communication using the ElGamal public key cryptosystem.*

(a) Alice choose $a = 947$ as her private key. What is the value of her public key A?

(b) Bob choose b =716 as his private key, so his public key is

$$B \equiv 2^{716} \equiv 469\,(mod\, 1373).$$

$m = 583$ using the ephemeral key $k = 887$. What is the ciphertext (c_1, c_2) that Alice sends to Bob ?

(c) *Alice decides to choose a new private key a = 299 with associated public keyA* $= 2^2 99 = 34(mod\,1373)$. *Bob encrypts a message using Alice's public key and sends her the ciphertext* $(c_1, c_2) = (661, 1325)$. *Decrypt the message.*

(d) *Now Bob chooses a new private key and publishes the associated public key B = 893. Alice encrypts a message using this public key and sends the ciphertext* $(c_1, c_2) = (693, 793)$ *to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem* $2^b = 893\,(mod\,1373)$ *and using the value of b to decrypt the message.*

solution

(a) $A \equiv 2^{947} \equiv 177\,(mod\,1373)$, so Alice's public key is A = 177 .

(b) $c_1 \equiv 2^{877} \equiv 719(mod\,1373)$ and $c_2 \equiv 583 \cdot 469^{877} \equiv 623(mod\,1373)$. Alice sends the ciphertext $(c_1, c_2) = (719, 623)$ *to Bob.*

(c) $(c_a^{-1}) \cdot\ c_2 \equiv (661^{299})^{-1} \cdot\ 1325 \equiv 645^{-1} \cdot\ 1325 \equiv 794.\ \ 1325 \equiv 332\,(mod\,1373)$. Thus the plaintext is m = 332. It turns out that the ephemeral key is $k = 566$, but Alice does not know this value.

(d) The solution to $2^b \equiv 893\,(mod\,1373)$ is $b = 219$, which is Bob's privatekey. It is now easy to decrypt,

$(c_1^a)^{-1}.c_2 \equiv (693^{219})^{-1}.793 \equiv 431^{-1}\,.793 \equiv 532\,.793 \equiv 365(mod\,1373).$

Thus Alice's message to Bob is m = 365. (The ephemeral key was k = 932.)

Theorem 3.4. *Let (n, e) be a public RSA key and D the corresponding private RSA key. Then*

$$(m^e)^d \ mod \ n = m$$

for any integer m *with* $0 \leq m < n$.

Proof. Since $ed \equiv 1 \bmod (p-1)(q-1)$, there is an integer l with

$$ed = 1 + l(p-1)(q-1).$$

Therefore

$$(m^e)^d = m^{ed} = m^{1+l(p-1)(q-1)} = m(m^{(p-1)(q-1)})^l.$$

It follows that

$$(m^e)^d \equiv m(m^{(p-1)(q-1)l}) \equiv m \ mod \ p.$$

If p is not a divisor of m, then this congruence follows from Fermat's little theorem. Otherwise, the assertion is trivial because both side of the congruence are 0 mod p. Analogously, we see that

$$(m^e)^d \equiv m \ mod \ q.$$

Because p and q are distinct prime numbers, we obtain

$$(m^e)^d \equiv m \ mod \ n.$$

□

3.4 Types of attacks

Cryptanalysis deals with the attacks on cryptosystems. To make attacks on cryptosystems more difficult, one can keep the cryptosystem secret. However, it is not clear how much security is really gained in this way because an attacker has many was of finding out which cryptosystem is used. He can try to tell from in-tercepted ciphertexts

and to abtain information from well informed people. Therefore, in public applications such as the internet the cryptosystems that are used are public. Only the (private) keys and the plaintexts are secret. However, cryptosystems used by the military or a secret service are mostly secret.

Here we assume that an attacker knows which cryptosystem is used. Only the (private) keys and the plaintexts are assumed to be secret.

Different attackers may have different knowledge and different abilities. There are the followinhg types of attacks.

$Ciphertext - only\, attack$: The attacker only knows a ciphertext. This is the weakest attack.

A simple ciphertext-only attack is the following. The attacker decrypts the ciphertext with all keys from the key space. He finds the correct plaintext among the few plaintexts that make sense. That attack is called exhaustive search. It works for cryptosystems with too small key spaces where the meaning of "too small" depends on the available computing power.

Other ciphertext-only attacks use statistical properties of the plaintext language. For example, if the Caesar cipher is used with a fixed key, then each plaintext letter is encrypted by a fixed ciphertext symbol. Therefore, the most frequently used plaintext letter corresponds to the most frequently used ciphertext symbol; the second most frequently used plaintext letter corresponds to the second most frequently used ciphertext symbol, etc. Likewise, the frequency of pairs, triplets, etc. of the plaintext language is repeated in the ciphertexts. Those statistical properties can be used to decrypt ciphertexts and to find keys.

known as plaintext attack :Known plaintext attack: The attacker knows a plaintext and the corresponding ciphertext or several such pairs. She tries to decrypt other ciphertexts. An example: Many letters end with "Sincerely yours". If the attacker knows the corresponding ciphertext, then she can mount a known plaintext attack.

Chosen plaintext attack : The attacker is able to encrypt plaintexts of his choice but does not know the decryption key. He tries to de- crypt other ciphertexts. In a public-key cryptosystem such an attack is always possible since the encryption key is publicly known. An example: The attacker intercepts a ciphertext. He knows that the corresponding plaintext is either "yes" or "no". To find out which plaintext was encrypted, he encrypts "yes" and he encrypts "no". Then he compares the two ciphertexts with the intercepted ciphertext.

Chosen ciphertext attack : The attacker can decrypt ciphertexts os his choice but does not know the decryption key. He tries to find the decryption key. For example, such an attack is possible if a cryptosys- tem is used for identification. This works as follows. Alice wants to make sure that she is connected to Bob. She sends an encrypted ran- dom number to Bob for which only Bob knows the decryption key. Bob decrypts the number and sends it back to Alice. This convinces Alice that she is connected to a person that knows the secret decryp tion key. She knows that this person is Bob. An attacker can try to impersonate Alice. Instead of sending random numbers to Bob he sends messages of his choice. Bob will have difficulties in detecting this.

There are *passive and active attackers*. A passive attacker can only mount cipher-only attacks. An active attacker can mount cho-

sen plaintext and chosen ciphertext attacks. He can also change the ciphertext in order to manipulate the corresponding plaintext.

Cryptography Algorithms	***File size (kilo bytes)***	***Encryption Time (in Seconds)***	***Decryption Time (in Seconds)***
DES	32	0.27	0.44
	126	0.83	0.65
	200	1.19	0.85
	246	1.44	1.23
	280	1.67	1.45
AES	32	0.15	0.15
	126	0.46	0.44
	200	0.72	0.63
	246	0.95	0.83
	280	1.12	1.10
RSA	32	0.13	0.15
	126	0.52	0.43
	200	0.74	0.66
	246	1.11	0.93
	280	1.39	1.23
ElGamal	32	0.45	0.43
	126	1.03	0.85
	200	1.41	1.13
	246	1.75	1.30
	280	1.83	1.64

Chapter 4

Applications

4.1 Applications Of Encryption:

Encryption plays a crucial role in cryptography, ensuring data security and confidentiality. Let's explore its significance:

1. **Confidentiality:**
   Encryption ensures that sensitive information remains private. By converting data into an unreadable format (ciphertext), only authorized individuals with the proper decryption key can access the original data. Examples include protecting personal messages, financial transactions, and sensitive files.

2. **Data Protection during Transmission:**
   When data is transmitted over networks (such as the Internet), encryption prevents interception by unauthorized parties. Secure communication protocols (e.g., HTTPS) use encryption to safeguard data during transmission.

3. **Password Security:**
   Encrypted passwords protect user accounts. Storing plaintext passwords is risky; encryption ensures that even if the password

database is compromised, attackers cannot easily retrieve the original passwords.

4. **Secure Storage:**
   Encryption secures data at rest (stored on disks or databases). Even if physical storage devices are stolen, the encrypted data remains inaccessible without the proper decryption key.

5. **Compliance and Regulations:**
   Many industries (e.g., healthcare, finance) have legal requirements for data protection. Encryption helps organizations comply with regulations (e.g., GDPR, HIPAA).

6. **Digital Signatures:**
   Encryption is used in digital signatures to verify the authenticity and integrity of messages. Digital signatures ensure that a message has not been altered and comes from a trusted source.

7. **Cloud Security:**
   Cloud providers use encryption to protect data stored in their services. Users can also encrypt data before uploading it to the cloud.

8. **Mobile Device Security:**
   Encryption secures data on mobile devices (phones, tablets). If a device is lost or stolen, encrypted data remains protected.

9. **Secure File Sharing:**
   Encrypted files can be safely shared with others. Only authorized recipients with the decryption key can access the content.

10. **Financial Transactions:**
    Online banking, e-commerce, and payment gateways rely on en-

cryption to protect financial transactions. SSL/TLS encryption secures credit card details during online purchases.

11. **Health Records and Personal Information:**
Medical records, personal identification, and other sensitive data are encrypted to prevent unauthorized access.

12. **Military and Government Communications:**
Encryption is crucial for secure military and government communications. It prevents adversaries from intercepting and deciphering sensitive information. In summary, encryption ensures data privacy, prevents unauthorized access, and plays a vital role in securing digital communication and storage.

13. **Blockchain encryption:**
The secure nature of blockchain means that the encryption of blockchain technology is very much a heightened security measure. Blockchain encryption is the prevention of sensitive information from getting into the wrong hands and being misused or forged. Because the nature of blockchain is very mich lies in data not being able to be edited or removed so the data must be very much protected. All the data is verified, uploaded and secured by way of encryption. The way that blockchain and encryption security works are based on an algorithm that must be solved as a way for a piece of data to be verified when it comes to being added to a blockchain. This ensures that security measures are taken before the stay is even stored.
The encryption itself, when it comes to blockchain, lies in the mathematics behind the mining network. Encryption is the process of converting information or data into a code especially to

prevent unauthorised access. Encryption uses more mathematical techniques along with passwords and keys used to decrypt the information and heavily relies upon an algorithm to make original information unreadable. The process itself converts the original information and data into plaintext which is an alternative text which allows it to be encrypted and secure. When an authorised user needs to access or read the data in a blockchain, they can decrypt it by using a key. This will then convert the plaintext back to the original text to be accessed, and this is very much the case with blockchain.

4.2 Disadvantages:

- **Speed:** Eneryption can slow down during the data transmission, taking longer than unencrypted messages.
- **Require a large amount of power:** Cryptography is computationally intensive, requiring large amounts of computing power to encrypt and decrypt data.
- **Vulnerable:** It is also susceptible to cryptographic attacks, such as brute force attacks, that can compromise the security of encrypted data.
- **Requiring a high skill:** Cryptography requires a high degree of skill, knoeledge and resources to implement correctlty.
- **Loss:** If the password or key lost, the user will be unable to open the encrypted file.

Chapter 5

Conclusion

With advancement in technology it becomes more easier to encrypt data, with neural networks it becomes easier to keep data safe. Neural networks of Google Brain have worked out to create encryption, without teaching specifics of encryption algorithm. Data Scientist and cryptographers are finding out ways to prevent brute force attack on encryption algorithms to avoid any unauthorized access to sensitive data.

Data protection is a function of encryption, and algorithm refers to a set of guidelines or remarks that must be followed to throughout the encryption process. The encryption functions, procedures, and keys utilised all contribute to the system's effectiveness. Using a public or private key, the recipient may transform the coded text or unreadable format back to plain text.

In this dissertation, we studied AES is resistant to all types of attacks except brute force attacks. Still, a lot of internet security experts think that AES will become the industry standard for private-sector data encryption in the future.

Bibliography

[1] Johannes A. Buchmann, Introduction To Cryptography, Second Edition, Springer, (2001).

[2] Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, An Introduction To Mathematical Cryptography, Springer, (2008).

[3] Wade Trappe and Lawwrence C. Washington, Introduction to Cryptography with Coding Theory, Second Edition,Pearson Education, Inc, (2006).

[4] Faiqa Maqsood, Muhammad Mumtaz Ali, Muhammad Ahmed and Munam Ali Shah, Cryptography: A Comparative Analysis for Modern Techniques, *International Journal of Advanced Computer Science and Applications,* 8(6), (2017).

[5] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[6] Haitham A. Anwer and Ali Abdulwahhab Mohammed, A New Method Encryption and Decryption, *webology, 18(1)*, January, (2021).