

PROFESSIONAL TRAINING REPORT
at
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the award of Bachelor in
Technology Degree in Information Technology

By
RAUSHAN KUMAR
Registration No.: 39120092



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY

JEPPIAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI-600119, TAMILNADU

NOVEMBER 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI

CHENNAI- 600119

www.sathyabama.ac.in



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **RAUSHAN KUMAR (Reg. No: 39120092)** who carried out the project entitled "**CRYPTOGRAPHY (CYBERSECURITY)**" under my supervision from June 2021 to November 2021.

Internal Guide

Dr. P. Jeyanthi

Submitted for Viva Voce Examination held on 07/11/2021

DECLARATION

I, **RAUSHAN KUMAR** hereby declare that the project entitled **CRYPTOGRAPHY (CYBERSECURITY)** completed by me under the guidance of **Dr.P.Jayanthi** is submitted in partial fulfilment of the requirements for the award of Bachelor in Technology Degree in Information Technology.

RAUSHAN KUMAR

DATE: 07/11/2021

DIGITAL SIGNATURE OF CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** at **Sathyabama Institute** for their encouragement and guidance in the completion of this project.

I would like to express my sincere gratitude to my Project Guide **Dr.P.Jeyanthi**, for her valuable guidance, suggestions and constant encouragement which paved the way for the successful completion of my project work.

I would also like to express my humble appreciation towards the staff over at **Cognibot Labs** & especially our trainer, **Vengatesh Nagarjan** who held a guiding hand at every turn throughout the completion of my Machine Learning course.

I wish to express my thanks to all teaching and non-teaching staff members of the **Department of Information Technology** who were helpful in many ways throughout the duration of the project.

TRAINING CERTIFICATE



CERTIFICATE OF COMPLETION

CSW-I-33-081121 is given to

RAUSHAN KUMAR

For completing the Cyber Security training that includes basics of Cyber Security, Pentesting, Networking, and WebApp.

Aaron V Sandeen

AARON SANDEEN
CEO - CSW

N. Vengatesh

VENGATESH NAGARAJAN
MENTOR

PREFACE

I have made this report file on the topic **Cryptography**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone

Has ended on a successful note. I express my sincere gratitude to my guide

Mrs.S.Jeyanthi and my teacher Vengatesh Nagarjan who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement,

confidence and most importantly the track for the topic whenever I needed it.

ABSTRACT

Many organizations are working hard to secure themselves from the growing threats of message hacking through various trends in cryptography. Yet the headlines are dominated with the latest news of message passing disaster more frequently than any time before.

This document intends to review this problem and propose several possible solutions. The cryptographic industry has been responding to these threats with ever-quicker responses to the rapid onslaught of malicious techniques, while corporations establish strict cryptographic techniques.

Placing organizations cryptographic techniques at the desktop level is like closing all the doors in a house.....while leaving windows and other entry points open. The present document discusses various cryptographic techniques of all times such as the three basic algorithms namely private key algorithm, public key algorithm and the hash functions. The need for having three encryption techniques has also been encrypted.

A detailed discussion has been done on the classical cryptography and the drawbacks of the classical cryptography to ensure the need for going to new trends in cryptography like *quantum cryptography*, *elliptic curve cryptography*. These new techniques that has emerged out of various exploitations in the field of cryptography rises a fair amount of hope that we can overcome the problems we are facing in a head hoc way.

These proven technologies can meet the needs of the most demanding of environments while their respective focus on manageability has automated many tasks and simplified administrative functions through easy-to-use interfaces developed through years of customer feedback. And at the end of the document we can conclude that soon we can save secrecy involved in message passing from the dangerous clutches of message hackers.

TABLE OF CONTENT		
Chapter No.	TITLE	Page no.
	ABSTRACT	
1	Introduction of Cryptography	1
1.1	About the concept	
1.2	Why we need cryptography	
1.3	Types of cryptography	
1.4	Cryptology	
2	Cryptographic Protocols	6
2.1	Introduction to Protocols	
2.2	Purpose of protocols	
2.3	Group of Actors	
2.4	Types of Protocols	
2.5	Attacks against Protocols	
2.6	Communication using Symmetric Cryptography	
2.7	Message Authentication Code	
2.8	Communication using Pubic Key Cryptography	
2.9	Digital Signatures	
2.10	Random and Pseudo Random sequence generation	
3	Aim And Scope of present investigation	10
3.1	Aim	
3.2	Scope	

4	METHODS OR ALGORITHMS USED	11
4.1	SOFTWARE REQUIREMENT	
4.2	ALOGRITHM USED	
5	PERFORMANCE METRICS AND RESULTS	14
6	Conclusion and Research	15
	REFERENCES	
	APPENDIX	
	CODE SCREENSHOT	
	OUTPUT SCREENSHOT	

CHAPTER 1

INTRODUCTION

1.1 ABOUT THE CONCEPT

The Internet or the global Internet is the internationally connected network of computer networks with addresses that are administrated by IANA (Internet address and Naming Authority). It grew dramatically because anyone can connect to it and anyone connected to it can connect others to it as well.

Each site that connected to it, can become an Internet Service provider to other sites Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography and new trends in use today.

I would like to say at the outset that this paper is very focused on terms, concepts, and schemes in current use and is not a treatise of the whole field.

1.2 Why do we need Cryptography?

Cryptography plays an important role in today's and future's confidential data communication. For example, communications over telephone lines including faxes and e-mail messages, financial transactions, medical histories, e-banking and even other types of important informations need secure communication medium. Sometimes, the medium is hacked by intruders and gets all of your information. Therefore, cryptographic applications provide the secure communication medium to transfer your data reliably, so that if any one tries to hack data, then it is not useful to him because the data is in encrypted form.

Cryptography is one of the tools, which ensures more privacy. The ability to encrypt data, communications and other information, gives individuals, the power to restore personal privacy. Cryptography protects the world's banking systems as well, which is the requirement of today's world. Many banks and other financial institutions conduct their business over open switched networks like Internet. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and rob banks without a trace.

1.3 Types of Cryptography

There are many types of cryptography, including codes, steganography, ciphers and mathematical algorithms. Codes rely on codebooks. Steganography relies on different ways to hide or disguise writing. Ciphers include both computer-generated ciphers and those created by encryption methods. Nowadays, mostly cryptographic algorithms are implemented on theories of mathematics. Number theory and Group theory are the most widely used in the computerized cryptographic algorithms. Following is the detail information about different types of cryptography.

Codes and Codebooks

A well-developed code can represent an idiom and entire sentences with symbols, such as three or four letters group. A properly constructed code can give a high degree of security but the more same codebook is used, the less secure it becomes

For example, imagine a codebook with two columns. In the first column, is a list of all the words that are commonly used in specific communication and in second column is a list of different words. In case of military usage codebook, it contains all the possible geographic areas in a region, all possible times and all military terms. To create a coded message, the encoder writes down the actual message. He then substitutes words in the codebook by finding matches in the second column for the words in the message and using the new words instead.

For example, suppose that the message is Attack the hill at dawn and the codebook contains the following word pairs: attack = stand, the = liquid, hill = ginger, at = chart, and dawn = close. The encoded message would read Stand liquid ginger chart close.

If the coded message fell into enemy's hands, the enemy would understand only that it was in code form, but without the codebook the enemy would have no way to decrypt the message. But there is problem with that technique; codebooks lose some of their importance over a time period. That

is, if the coded message fell into enemy hands and on the next day the hill was attacked at dawn, the enemy could link the event to the coded message. If another message containing the word ginger was captured and that particular day something else happened on the hill, the enemy could assume that ginger = hill is in the codebook. Over time, the enemy cracks the code. So, the codebook's code is necessarily changed after used for securing communication

Steganography

Steganography is an ancient Egyptian technique of hiding the message using liquid like invisible inks, microscopic writing and hiding code words within sentences of a message. Cryptographers may apply steganography to electronic communications and that application is called transmission security

The ancient Greeks and Romans, as well as other empires at around the same time, used the forms of steganography. The invention of the first shorthand system was presumably intended as a form of secret writing. Hidden messages were also sent, using invisible ink in which they used citric acid juice like Orange, Lemon and Vinegar etc. as ink and written on a plain sheet. The written message could not be read unless that paper was put into hot or warm place. Microscopic writing is an art in which the writing is so small so that nobody can read it easily.

Cipher

The word "cipher" means "secret" and it is the most popular and secure technique as compared with codes and codebooks as well as steganography. Ciphers are the secret codes used to encrypt plaintext messages. There are two general types of ciphers, namely Substitution and Transposition ciphers [3].

In substitution cipher, an alphabet is to replace plaintext with other letter or symbol. In transposition ciphers, the mix up of letters in a word or sentence is made to convert it into unintelligible form.

We also have computer ciphers that are used for digital messages encryption. Computer ciphers differ from ordinary substitution and transposition ciphers in which a computer application performs the encryption of data. Below is the more detail description of substitution and transposition ciphers.

a) Substitution Cipher

In simple substitution ciphers, an alphabet or symbol is substituted for each single or multiple letters. For example, a substitution cipher was devised long ago by Julius Caesar, which shifted all the letters in the alphabet by three places. To express Caesar's cipher mathematically, first replace each letter by an integer from 1 to 26, based on its position in the alphabet. That is 'A' is replaced by 1, 'B' by 2, 'C' by 3 and so on. Caesar cipher is represented by function f that has non-negative integer value 'a', where 'a' less than or equal to 26 [3], [5].

$$f(a) = (a+3) \bmod 26$$

Thus, when the letter 'a' is substituted, d is used, and when 'b' is to be written, 'e' is used and so on. The letters wrap around at the end of the alphabet. So,

if a person wants to encipher 'z', it is written as 'c' by taking modular 26. Similarly, 'y' is written as 'b'. The entire cipher is represented by two rows of letters. These rows are called a lookup table.

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

When someone wants to encrypt a word, he or she looks up the original letter in the top row and uses the corresponding ciphertext letter in the bottom row. For example, secret message produced from the message "ATTACK THE HILL" using the Caesar cipher is "DWWDFN WKH KMOO".

While the above substitution cipher is easy to remember, it is also easily breakable. To make a substitution cipher more complex, multiple substitutions and sometimes even numbers are added to the cipher.

In multiple substitution (poly-alphabetic) ciphers, a keyword or number is employed. The first message letter might be enciphered by adding to it the numerical value of the first letter of the keyword, the second message letter is enciphered similarly, using the second letter of the keyword and so on, repeating the keyword as often as necessary to encipher the whole message. When adding the numerical value of a keyword letter to a message letter, one starts counting with the message letter. Thus, to encipher the word TODAY by the code word DIG, t becomes w, as d is the fourth letter of the alphabet (count t, u, v, w); o becomes w, as i is the ninth letter of the alphabet; and d becomes j, as g is the seventh letter of the alphabet. For the rest of the message the code word is repeated, and thus TODAY is coded WWJDG [52].

There are also other types of poly alphabetic substitution ciphers exist in which the most common and reoccurring word is replaced by single or double letters. For example, "this" is replace by 't'; "is" by 's' and "secret" by "se", so that the sentence "this is secret" in cipher form looks "t s se".

b) Transposition Cipher

In a transposition cipher, the order of plaintext alphabets is changed to get the ciphertext. The message is usually written without word divisions in rows of letters arranged in a rectangular block. The letters are then transposed in a prearranged order, such as by vertical columns, diagonals, or spirals, or by more complicated systems [3], [52].

The arrangement of the letters in the enciphered message depends upon the size of the block of code words used and upon the route followed in inscribing and transposing the letters.

A cipher in which every pair of letters is swapped is an example of a transposition cipher. For example, the ciphertext for "cryptography" would be "rcpyotrgpayh".

The first and second letters are swapped then the third and fourth letters are swapped and so on. A more complex transposition cipher technique is to write the message in a rectangular form, row by row and read the message off, column by column but permute the order of the columns. The order of the columns then becomes the key to the algorithm or you assign your own key. This key again use in decrypting the ciphertext [3]. For example, we have plaintext "attack the hill at dawn" is encipher as

Key	1	2	3	4	5
-----	---	---	---	---	---

Plaintext:	a	t	t	a	c
	K	t	h	e	h
	l	1	1	a	t
	d	a	w	n	a

Cipher text: akidttlathlwaeanchta

In this type of transposition cipher, all the columns entries must be filled by alphabet of sentence, if there is empty space remaining in last row then it is filled by a, b, c and so on. Transposition ciphers may be combined with substitution ciphers to produce a more complex encoded message

1.4 Cryptology

The branch of mathematics encompassing both cryptography and cryptanalysis is called cryptology and its practitioners are cryptologists. We have already discussed about cryptography, so we now talk about cryptanalysis. Cryptanalysis is the study of mathematical techniques for attempting to defeat cryptographic techniques and more generally, the art and science of breaking ciphertext without the knowledge of proper method of decryption. A cryptanalyst is a person or machine that engages in cryptanalysis

Independent Study Report - Cryptography Cryptanalysis is the art of analyzing cipher text to take out the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers. Understanding the process of code breaking is very important when designing any encryption system. Current systems require very powerful computer systems to encrypt and decrypt data. While cryptanalysis has improved as well, some systems may exist that are unbreakable by today's standards. Some cryptographers believe that the National Security Agency (NSA) of the United States has enormous, extremely powerful computers that are entirely devoted to cryptanalysis.

The Caesar's cipher that described above is easy to break. Because the encryption and decryption algorithm are known and there are only 25 keys to try. Before computers technology, experts of cryptanalyst would look at cipher text and tried their guesses as to which letters were substituted for which other letters .

Early cryptanalysis techniques included computing the frequency with which letters occur in the language that is being intercepted. For example, in the English language, the alphabets e, s, t, a, m, and n occur much more frequently than do q, z, x, y, and w. So, cryptanalysts look at the ciphertext for the most frequently occurring letters and assign them as candidates to be e, s, t, a, m, and n. Cryptanalysts also know that certain combinations of letters are more common in the English language than others. For example, 'q' and 'u', 't' and 'h' occur together. The frequency and combinations of letters help cryptanalysts build a table of possible solution letters.

Cipher text that is produced using different keys and frequently changed keys makes the cryptanalyst's task of code breaking difficult.

CHAPTER - 2

Cryptographic Protocols

2.1 Introduction to Protocols

A protocol is the process of sequence of steps involving atleast two or more parties to complete the communication task. A single person can perform a sequence of steps to achieve a task but this is not a protocol because for protocol, it is necessary that at least two people must be engage in a process.

Protocols have some other characteristics as well:

- In starting, all the parties that involve in the protocol compulsorily know the all steps and sequence that occur in it.
- All parties must be agreeing to follow the sequence of steps.
- All the steps must be defined clearly so that no chances remain for misunderstanding.
- At every step, there must be a specified action performed.

2.1.1 Cryptographic Protocol

A cryptographic protocol is a protocol that uses in cryptography. The parties that involve in it can be trust each other or may not be. In cryptographic protocols, there is cryptographic algorithm is used for secure communication. The main point of using cryptography in a protocol is to prevent or detect eavesdropping, hacking and cheating.

2.2 Purpose of Protocol

Nowadays, more and more human interaction takes place over computer networks instead of direct communication. It is unfair to suppose that people on computer networks are honest. Most are honest but the few dishonest can do a lot of damage in computer networking. By formalizing protocols, we can look at ways in which dishonest parties can weaken them [2].

2.3 Group of Actors

For the explanation of communicating protocols, there is list of some actors whose role defines in table 2.1 below. These names are used worldwide in the explanation of cryptographic protocols. For example, Alice and Bob are the first two persons and they will perform all two-person protocols. According to a rule, Alice will initiate all protocols and Bob will respond. If the protocol requires a third or fourth person, Carol and Dave will perform those roles. Other actors will also play specialized supporting roles whenever their need. Different actor's introduced below

2.4 Types of Protocols

Well, there are a lot of types of protocol exist in studying cryptography while three main types of protocol discuss below [2].

Arbitrated Protocols

An arbitrator is a disinterested third party trusted to complete a protocol task. Disinterested means that the arbitrator has no keen interest in the protocol and no particular reliability to any of the parties involved. Trusted means that all people involved in the protocol accept the arbitrator orders. Arbitrators can help complete protocols between two mutually distrustful parties.

In the real world, lawyer (Trent) role is as arbitrator. For example, Alice is selling her home to Bob, he is a stranger for her. Bob wants to pay by check but Alice has no way of knowing if the check is fine or not. Alice wants the check to clear before she gives the home registry paper to Bob. Bob, who doesn't trust Alice and not want to handover a check without receiving the home papers.

Both parties trusted on lawyer trusted. So, with the help of him, Alice and Bob can use the following protocol to ensure that neither cheats each other:

- (1) Alice gives the home's paper to the lawyer.
- (2) Bob gives the check to Alice in the presence of lawyer.
- (3) Alice deposits the check.
- (4) After a specified period for the check to clear, the lawyer gives the home's paper to Bob.
- (5) If the check does not clear within the specified time period, Alice shows proof of this to the lawyer and the lawyer returns the papers to Alice.

In this protocol, Alice trusts the lawyer not to give Bob the home property papers unless the check has cleared and to give it back to her if the check does not clear. Bob trusts the lawyer to hold the home's paper until the check clears and to give it to him. The lawyer doesn't care if the check clears or not. He will do his part of the protocol in either case because both parties will pay him in either case.

In the above example, the lawyer is playing the part of an escrow agent. Lawyers also act as arbitrators for wills and sometimes for contract negotiations. The various stock exchanges act as arbitrators between buyers and sellers.

Adjudicated Protocols

Due to the high cost of hiring arbitrators (lawyer), arbitrated protocols can be subdivided into two subprotocols. One is a nonarbitrated subprotocol, executed every time parties want to complete the protocol. The other is an arbitrated subprotocol, executed only in exceptional conditions when there is a dispute. This special type of arbitrator is called an adjudicator.

An adjudicator is also a disinterested and trusted third party protocol. Unlike an arbitrator, he is not directly involved in every protocol. The adjudicator is called in only to determine whether a protocol was performed fairly or not.

For example, Judges are also adjudicators. A judge is brought in only if there is a dispute. Alice and Bob can enter into a contract without a judge. A judge

never sees the contract until one of them hauls the other into court. This contract signing protocol can be formalized in this way:

Nonarbitrated subprotocol (executed every time):

- (1) Alice and Bob discuss the terms of the contract.
- (2) Alice signs the contract.
- (3) Bob signs the contract.

Adjudicated subprotocol (executed only in case of a dispute):

- (4) Alice and Bob appear before a judge.
- (5) Alice presents her evidence.
- (6) Bob presents his evidence.
- (7) The judge rules on the evidence.

The difference between an adjudicator and an arbitrator is that the adjudicator is not always necessary. In a dispute, a judge is called in to adjudicate. If there is no dispute, using a judge is unnecessary. There are adjudicated computer protocols. These protocols rely on the parties to be honest; but if someone suspects cheating, a body of data exists so that a trusted third party could determine if someone cheated. In a good adjudicated protocol, the adjudicator could also determine the cheater's identity. Instead of preventing cheating, adjudicated protocols detect cheating. The inevitability of detection acts as a preventive and discourages cheating

Self-Enforcing Protocols

A self-enforcing protocol is the simplest type of protocol. This protocol is itself assurance fairness. Neither arbitrator nor adjudicator is required to complete the protocol or resolve disputes. In this case, if any one of the parties tries to cheat, the other party immediately detects the cheating and the protocol working is stopped.

2.5 Attacks against Protocols

Different types of intruder can try various ways to attack a protocol. An attack, in which the attacker just observing the communications is called a passive attack, in that case the attacker does not affect the protocol. All he can do is just observe the protocol and attempt to gain information. Passive attacks are difficult to detect but easier to prevent it.

Another type of attack in which an attacker could try to alter the protocol to destroy the communication or introduce new messages in the protocol, delete existing messages, substitute one message for another, replay old messages, interrupt a communications channel, or alter stored information in a computer. These are called active attacks because they require active involvement

Active attacks are easy to detect but difficult in prevention. Active attacks are much more serious, especially in protocols in which the different parties don't necessarily trust one another..

2.6 Communication using Symmetric Cryptography

The two parties wanted to encrypt their communications. Let's see, Alice want to send an encrypted message to Bob.

- (1) Alice and Bob agree on a cryptographic algorithm.
- (2) Alice and Bob agree on a key.
- (3) Alice takes her plaintext message and encrypts it using the encryption algorithm and the key. This creates a ciphertext message.
- (4) Alice sends the ciphertext message to Bob.
- (5) Bob decrypts the ciphertext message with the same algorithm and key and reads that message.

Independent Study Report - Cryptography With a symmetric algorithm, Alice and Bob can perform step 1 in anywhere but they must perform step 2 in secret because the key must remain secret until the communication is not end. If someone gets this key, he easily read his or her message

2.7 Message Authentication Code

A message authentication code (MAC) is also known as a data authentication code (DAC), is a one-way hash function with the addition of a secret key algorithm. The hash value is a function of both the pre-image and the key. The theory is exactly the same as hash functions, except only someone with the key can verify the hash value. You can create a MAC out of a hash function or a block encryption algorithm .

2.8 Communications Using Public-Key Cryptography

Whitfield Diffie and Martin Hellman described **public-key cryptography** concept in 1976. They used two different keys one public and the other private. It is computationally hard to deduce the private key from the public key. Anyone with the public key can encrypt a message but not decrypt it. Only the person with the private key can decrypt the message.

This is show you how Alice can send a message to Bob using public-key cryptography:

- (1) Alice and Bob agree on public-key cryptography.
- (2) Bob sends to Alice his public key.
- (3) Alice encrypts her message using Bob's public key and sends it to Bob.
- (4) Bob decrypts Alice's message using his private key.

Public key cryptography reduces the key management problem as in symmetry key algorithm. Due to two different keys used for encryption & decryption, especially the decryption key called private key is only having receiver end and it is not shared with anyone. So, only the correct receiver having private key can decrypt the message. If Mallory (Hacker) catches public key (which is shared key) and tries to decrypt the message, he will not succeed in it.

2.9 Digital Signatures

A digital signature is a kind of ID. You can use it on the Internet to identify yourself in a secure manner. This is extremely useful in areas such as electronic commerce. For instance, when making a credit card purchase on the Internet, you can use your digital signature to "sign" that purchase. This helps to ensure that only you can make purchases with your credit card number.

Digital Signatures are a central component of modern cryptographic systems. In analogy to handwritten signatures on paper documents, digital signatures are used to guarantee the authenticity of electronic documents. Thus they play an important role for example in secure and reliable systems for electronic commerce.

Applying an algorithm and the sender's private key to some or all of the message contents generates a digital signature in the form of a code. The recipient verifies the signature by decrypting it using the sender's public key.

2.10 Random and Pseudo-Random-Sequence Generation

Random-number generators are not random because they don't have to be. Most simple applications, like computer games, need so few random numbers that they hardly notice. However, cryptography is extremely sensitive to the properties of random-number generators. Use a poor random-number generator and you start getting weird correlations and strange results. If you are depending on your random-number generator for security, weird correlations and strange results are the last things you want.

CHAPTER 3

Aim And Scope of present investigation

3.1 AIM

The purpose of cryptography is to protect data transmitted in the likely presence of an adversary. A cryptographic transformation of data is a procedure by which plaintext data is disguised, or encrypted, resulting in an altered text, called ciphertext, that does not reveal the original input. The ciphertext can be reverse-transformed by a designated recipient so that the original plaintext can be recovered. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

3.2 SCOPE

While talking about information system, cryptography in computer science takes

major roles. In modern days, cryptography is considered to be technical practice of converting any readable text or message to a code which is an unintelligible one.

However, this coded message can be converted to its readable format with the help of cryptography. As computer system is becoming too complex, cryptography holds much importance and the skill of cryptography is deeply rooted in a subjected matter of computer science. Here are few scopes for cryptography students in computer science subject.

Cryptography holds four fundamental pillars which include authenticity, integrity, non-repudiation and confidentiality. Cryptography maintains the confidentiality of the data transferred through computer network by restricting audience except for the intended one. Cryptography can allow the user's identification before transmitting any data. Cryptography allows non-repudiation by restricting the option where the user can deny to the actions.

Cryptography ensures integrity of the user by analyzing the authentication of the same. For example; electronic signature is based on cryptographic tool which is considered to be a public key. One of the most important functions of cryptography is to maintain the integrity of the user in computer network

CHAPTER 4

METHODS OR ALGORITHMS USED

3.1 SOFTWARE REQUIREMENT

- ☐ Windows/Mac Based System
- ☐ Necessary Python Libraries

3.1.1 Windows/Mac System

Windows or Mac operating based system for personal computers or any other internet of things devices.

3.2 ALOGRITHM USED

Shift Cipher

The Caesar Cipher is a type of **shift cipher**. Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. The Shift Cipher has a **key K**,

which is an **integer from 0 to 25**. We will only share this key with people that we want to see our message.

How to Encrypt:

For every letter in the message **M** :

1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number **X**.

(A=0, B=1, C=2, ..., Y=24, Z=25)

2. Calculate: **$Y = (X + K) \bmod 26$**

3. Convert the number **Y** into a letter that matches its order in the alphabet starting from 0.

(A=0, B=1, C=2, ..., Y=24, Z=25)

For Example: We agree with our friend to use the Shift Cipher with **key K=19** for our message.

We encrypt the message "**KHAN**", as follows:

ENCRYPTION

	K	H	A	N
	10	7	0	13
+	19	19	19	19
(	29	26	19	32)
	3	0	19	6
	D	A	T	G

So, after applying the Shift Cipher with key K=19 our message text "**KHAN**" gave us **cipher text "DATG"**.

We give the message "DATG" to our friend.

How to decrypt:

For every letter in the cipher text **C** :

1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number Y.

(A=0, B=1, C=2, ..., Y=24, Z=25)

2. Calculate: **$X = (Y - K) \bmod 26$**

3. Convert the number **X** into a letter that matches its order in the alphabet starting from 0.

(A=0, B=1, C=2, ..., Y=24, Z=25)

Our friend now decodes the message using our agreed upon **key K=19**. As follows:

DECRYPTION

	D	A	T	G
	3	0	19	6
-	19	19	19	19
(	-16	-19	0	-13
	10	7	0	13
	K	H	A	N

So, after decrypting the Shift Cipher with key K=19 our friend deciphers the cipher text "**DATG**" into the message text "**KHAN**".

Why is the Shift Cipher insecure?

A cipher should prevent an attacker, who has a copy of the cipher text but does not know the key, from discovering the contents of the message. Since **we only have 26 choices for the key**, someone can easily try all of the 26 keys, one by one, until they recover the message. This type of attack is called a **brute force attack**.

CHAPTER 5

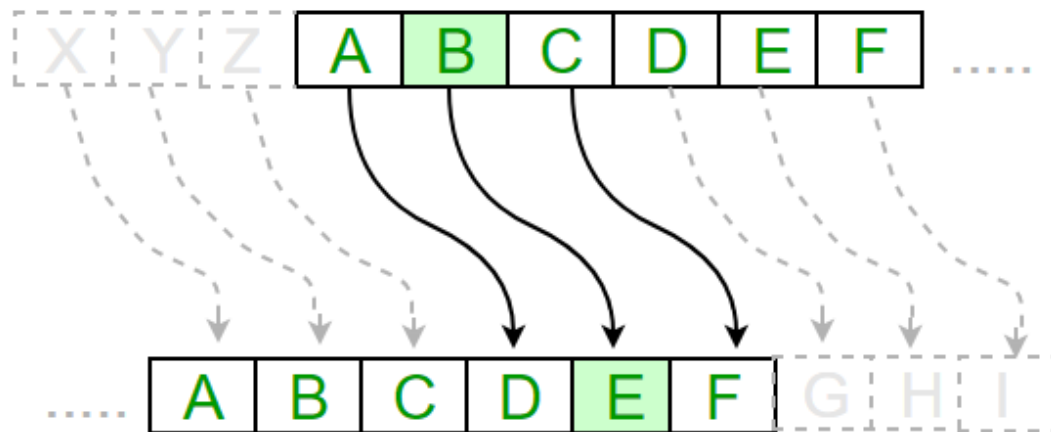
PERFORMANCE METRICS AND RESULTS

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.

Encryption of a letter by a shift n can be described mathematically as.



Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNQPQRSTUVWXYZ

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

CHAPTER 6

Conclusion and Research

7.1 Observations on Cryptography

If we want to find information about “What is cryptography”, then we can get a lot of data on this topic. But if we try to understand the concept of advance cryptography, then it is not an easy task. Many books and Internet URL resources are available on cryptography, which describes the types of algorithms, how they work, how they are made or implemented, how much secure they are etc. Cryptography is not the name of a single topic; there are a lot of topics existing in it. Cryptography is not just a single topic; it is a very vast subject on which a lot of research has been done, and this research is endless with new ideas cropping up from time to time.

Security problem is not today’s discovery. It is very old concept and due to computer technology changing very fast, therefore security importance is demanded more than other technologies in computer world. Cryptographic research is not today’s buzzword; it is one of oldest field around 4000 years ago. People, especially military of ancient Egyptian started working on it and today at the end of year 2004, still students, teachers, scientists are doing research on it throughout the world.

After reading cryptographic books, searching URLs and reading white papers of different scientists, I conclude following main points related to cryptography.

- Cryptography has a very old history, 4000 years ago. People try to do safe communication with collaborator because they also prevent their secrets from their enemies.
- The need of cryptography is to secure, reliable, authenticated information available whenever user want. Just like stamps made by different authorities to verify there messages or letters. This technique is still used for authentication in many areas like attestation of photocopies of original documents.

- Whenever a secret technique is exposed, its secretness will be cracked in some time. Therefore, secure communication problem has never been solved until or unless you must update yourself and your systems with latest security tools.
- Substitution and transposition cipher is now historic security technique. But when these were invented, everyone thought that it was very much secure and shall remain secure forever. But latest research has cracked this ciphertext. But at old times, these cipher techniques had great importance and mostly used by military. In Roman Empires, these techniques were used frequently.
- Steganography, the art of hiding the original text message, was still in use in different fields, but not in secure communication.
- Mathematics plays a vital role in the research of cryptography. Now, cryptology is defined, as the branch of mathematics deals with the study of encryption of data, to convert it into unintelligible form and only available for valid users.
- After the invention of computers especially computer network system, the importance of cryptography has increased more and more and as hacking, viruses, cracking etc. have become nuisance for computers.
- For many years, computers (computer networks) were used by U.S. military, but now it is more common in every day life. After Internet was invented, its use has increased day by day. Many big organizations, especially banks, corporate and finance sectors connect with their

REFERENCES

- Cryptography, <http://www.wikipedia.org/wiki/Cryptography>
- www.google.com
- www.geeksforgeeks.com
- Cognibot lectures & recorded sessions

APPENDIX:

CODE SCREENSHOT

```
code - Notepad
File Edit Format View Help
def machine():
    # creating key strings
    keys = 'abcdefghijklmnopqrstuvwxyz !'
    # auto generating the vaules of strings
    # value will be generted by taking last to first
    # concatinated with the rest of the string
    values = keys[-1] + keys[0:-1]
    # print(keys)
    # print(values)

    # creating two dictionaries
    encrytdict = dict(zip(keys, values))
    decryptdict = dict(zip(values, keys))

    # user input
    message = input("Enter your secret message: ")
    mode = input("Crypto Mode : Encode(E) OR Decode(D)")

    #encode and decode
    if mode.upper() == 'E':
        newMessage = ''.join([encrytdict[letter]
                               for letter in message.lower()])
    elif mode.upper() == 'D':
        newMessage = ''.join([decryptdict[letter]
                               for letter in message.lower()])
    else:
        print("Please try again, wrong choice entered")

    return newMessage.capitalize()

print(machine())
```

OUTPUT SCREENSHOT

```
Command Prompt
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nisch>md desktop
A subdirectory or file desktop already exists.

C:\Users\nisch>cd desktop

C:\Users\nisch\Desktop>code.py
Enter your secret message: hello
Crypto Mode : Encode(E) OR Decode(D)d
Ifmmp

C:\Users\nisch\Desktop>code.py
Enter your secret message: Ifmmp
Crypto Mode : Encode(E) OR Decode(D)e
Hello

C:\Users\nisch\Desktop>
```

