TY BSC(IT)

SEM 5

COMPILED BY

PROF. Tirup Parmar

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

NETWORK SECURITY - Syllabus

Unit I

1. Computer Security
   - Introduction
   - Need for security
   - Principles of Security
   - Types of Attacks
2. Cryptography
   - Plain text and Cipher Text
   - Substitution techniques
   - Caesar Cipher
   - Mono-alphabetic Cipher
   - Polygram
   - Polyalphabetic Substitution
   - Playfair
   - Hill Cipher
   - Transposition techniques
   - Encryption and Decryption
   - Symmetric and Asymmetric Key Cryptography
   - Steganography
   - Key Range and Key Size
   - Possible Types of Attacks

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

SECURITY MODELS

1. No Security

IN THIS SIMPLEST CASE, THE APPROACH COULD BE A DECISION TO IMPLEMENT NO SECURITY AT ALL.

2. Security through Obscurity

In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

3. Host Security

IN THIS SCHEME, THE SECURITY FOR EACH HOST IS ENFORCED INDIVIDUALLY.
THIS IS A VERY SAFE APPROACH, BUT THE TROUBLE IS THAT IT CANNOT SCALE WELL. THE COMPLEXITY AND DIVERSITY OF MODEM SITES/ORGANIZATIONS MAKES THE TASK EVEN HARDER.

4. Network Security

HOST SECURITY IS TOUGH TO ACHIEVE AS ORGANIZATIONS GROW AND BECOME MORE DIVERSE.
IN THIS TECHNIQUE, THE FOCUS IS TO CONTROL NETWORK ACCESS TO VARIOUS HOSTS AND THEIR SERVICES, RATHER THAN INDIVIDUAL HOST SECURITY.
THIS IS A VERY EFFICIENT AND SCALABLE MODEL.

TIRUP PARMAR

Computer Security

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically :

protected for three reasons:

01

To prevent theft of or damage to the hardware

02

To prevent theft of or damage to the information

03

To prevent disruption of service

Strict procedures for access to the machine room are used by most organizations, and these procedures are often an organization's only obvious computer security measures.
Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure.
Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

TIRUP PARMAR

1

CONFIDENTIALITY

The principle of *confidentiality* specifies that only the sender and the intended recipient(s) should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access a message.

Interception causes loss of message confidentiality.

2

AUTHENTICATION

Authentication mechanisms help establish **proof of identities.** The authentication process ensures that the origin of an electronic message or document is correctly identified.

Fabrication is possible in absence of proper authentication mechanisms.

3

When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the *integrity* of the message is lost.

Modification causes loss o f message integrity

4

NON-REPUDIATION

There are situations where a user sends a message, and later on refuses that she had sent that message.

5

The principle of access control determines who should be able to access what.

6

AVAILABILITY

The principle of *availability* states that resources (i.e. information) should be available to authorized parties at all times.

OSI standard for Security Model

- Authentication
- Access control
- Non-repudiation
- Data integrity
- Confidentiality
- Assurance or availability
- Notarization or signature

TIRUP PARMAR

WHY DO WE NEED SECURITY?

IN THE EVER CHANGING WORLD OF GLOBAL DATA COMMUNICATIONS, INEXPENSIVE INTERNET CONNECTIONS, AND FASTPACED SOFTWARE DEVELOPMENT, SECURITY IS BECOMING MORE AND MORE OF AN ISSUE. SECURITY IS NOW A BASIC REQUIREMENT BECAUSE GLOBAL COMPUTING IS INHERENTLY INSECURE. AS YOUR DATA GOES FROM POINT A TO POINT B ON THE INTERNET, FOR EXAMPLE, IT MAY PASS THROUGH SEVERAL OTHER POINTS ALONG THE WAY, GIVING OTHER USERS THE OPPORTUNITY TO INTERCEPT, AND EVEN ALTER IT. IT DOES NOTHING TO PROTECT YOUR DATA CENTER, OTHER SERVERS IN YOUR NETWORK, OR A MALICIOUS USER WITH PHYSICAL ACCESS TO YOUR ENGARDE SYSTEM.

PRINCIPLES OF SECURITY

Let us assume that a person A wants to send a check worth $100 to another person B. Normally, what are the factors that A and B will think of, in such a case? A will write the check for $100, put it inside an envelope, and send it to B.

1. A will like to ensure that no one except B gets the envelope, and even if someone else gets it, he/she does not come to know about the details of the check. This is the principle of **confidentiality.**

2. A and B will further like to make sure that no one can tamper with the contents of the check (such as its amount, date, signature, name of the payee, etc.). This is the principle of **integrity.**

3. B would like to be assured that the check has indeed come from A, and not from someone else posing as A (as it could be a fake check in that case). This is the principle of **authentication.**

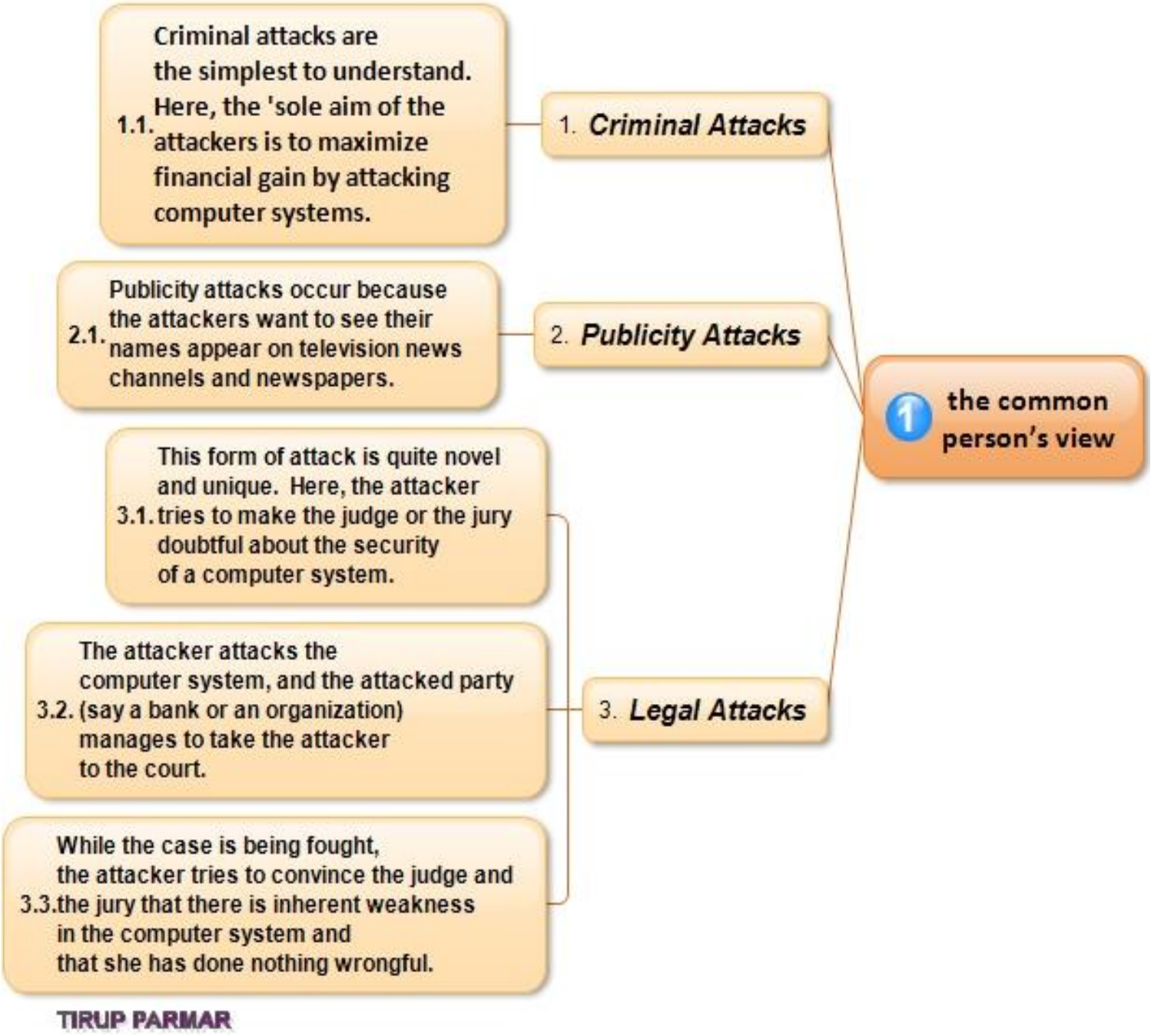
4. What will happen tomorrow if B deposits the check in his/her account, the money is transferred from A's account to B's account, and then A refuses having written/sent the check? The court of law will use A's signature to disallow A to refute this claim, and settle the dispute. This is the principle of **non-repudiation.**

These are the four chief principles of security.

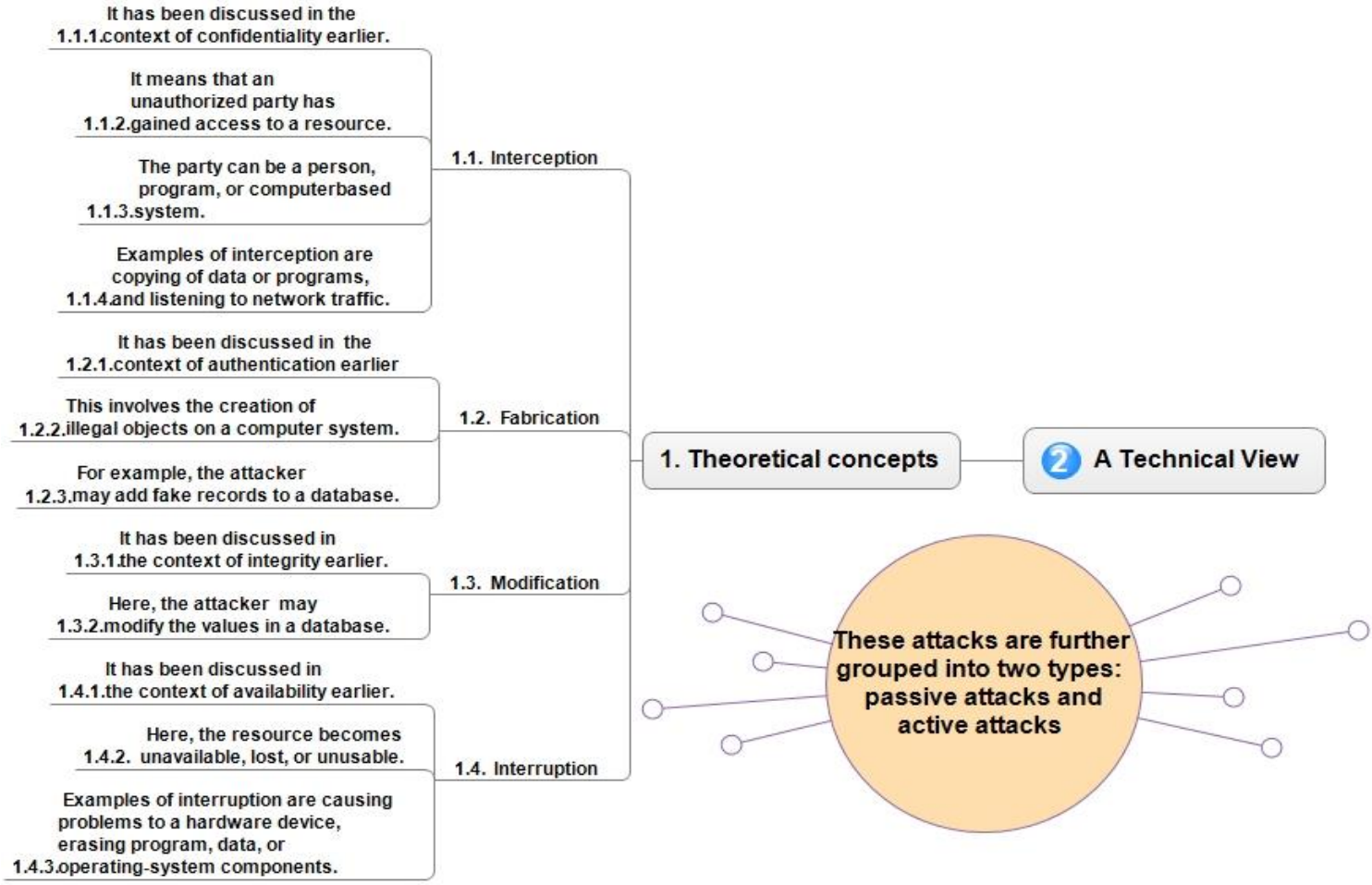
There are two more: **access control** and **availability,** which are not related to a particular message, but are linked to the overall system as a whole.

TIRUP PARMAR

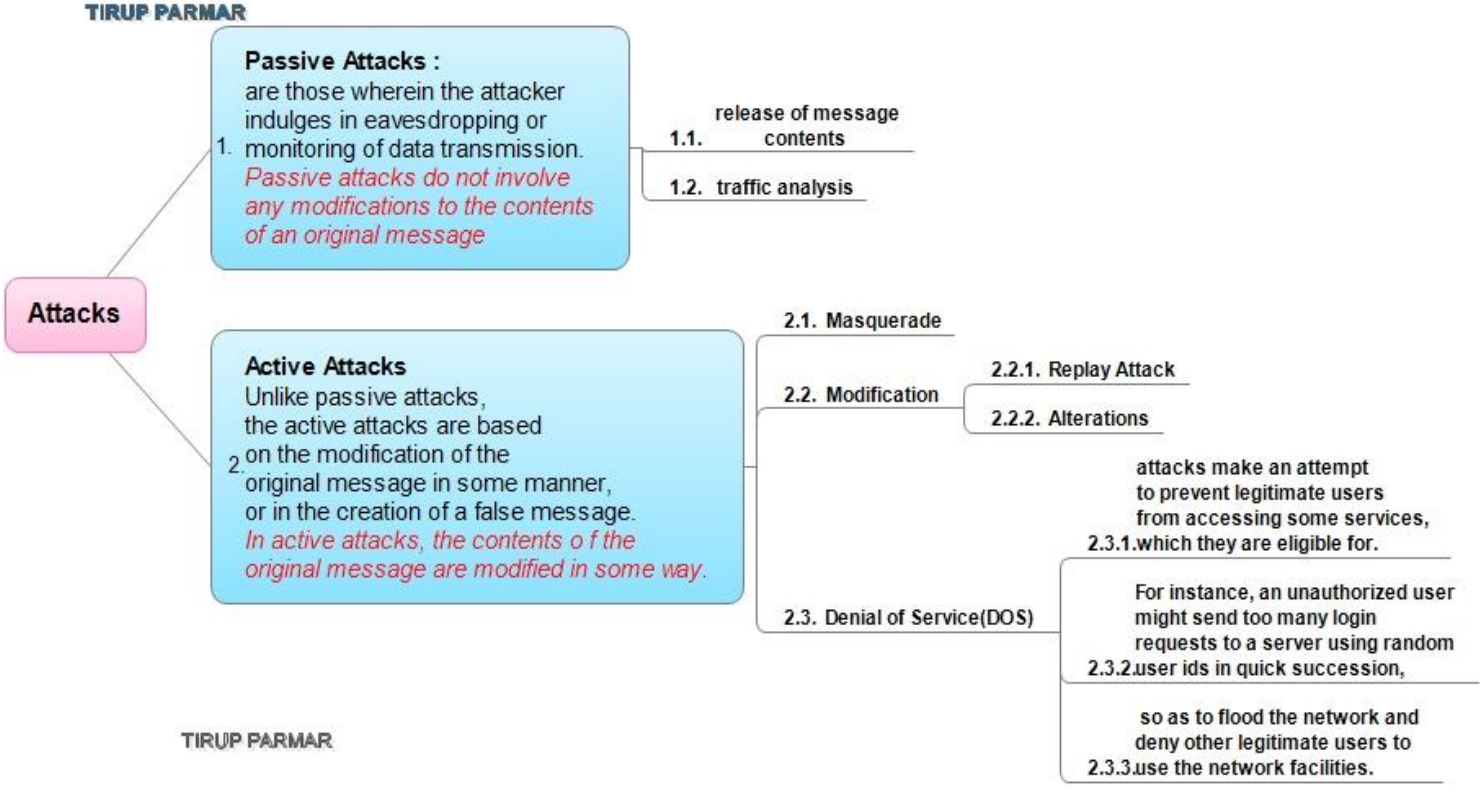
TYPES OF ATTACKS



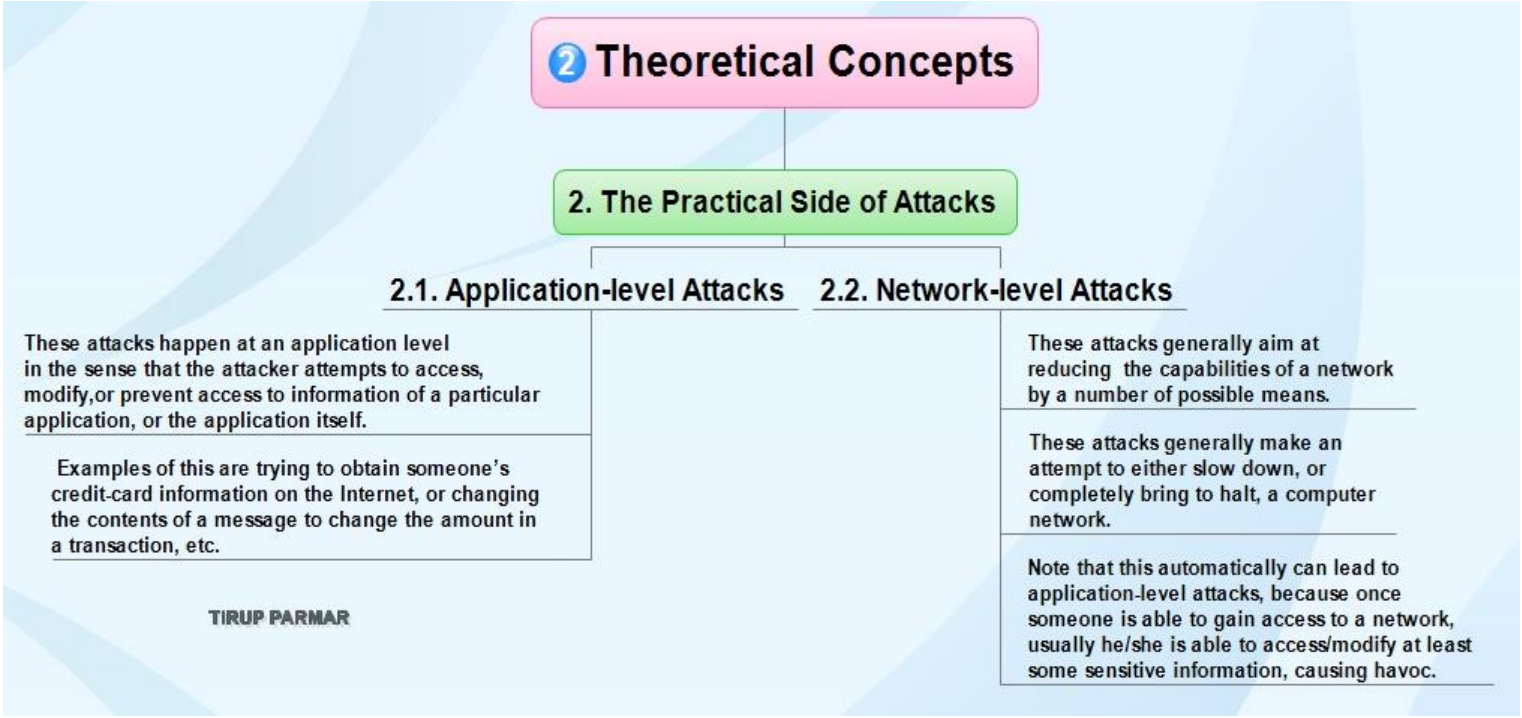
TIRUP PARMAR



TIRUP PARMAR



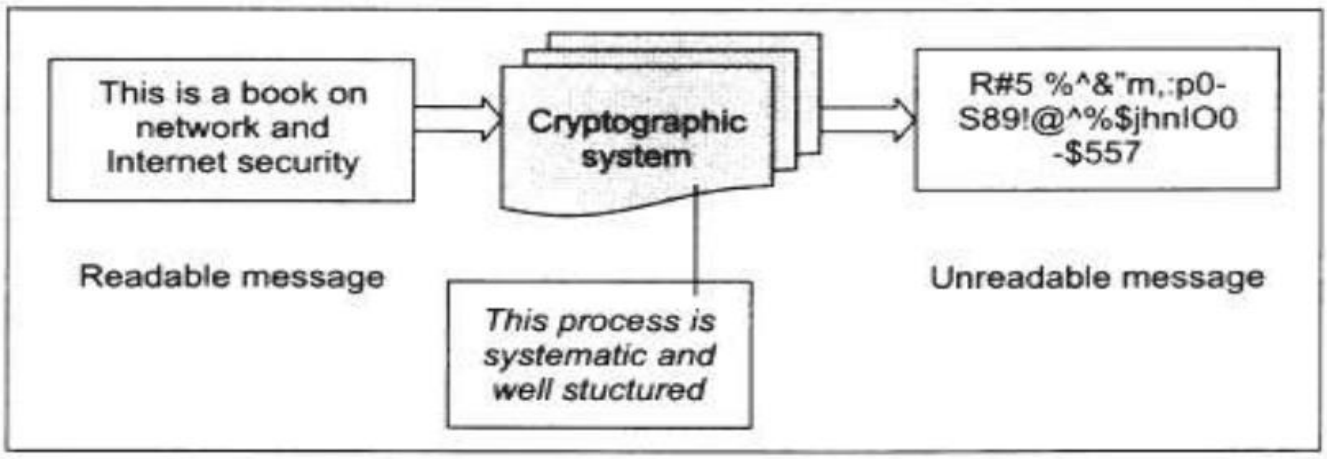
TIRUP PARMAR



CRYPTOGRAPHY TECHNIQUES

Cryptography

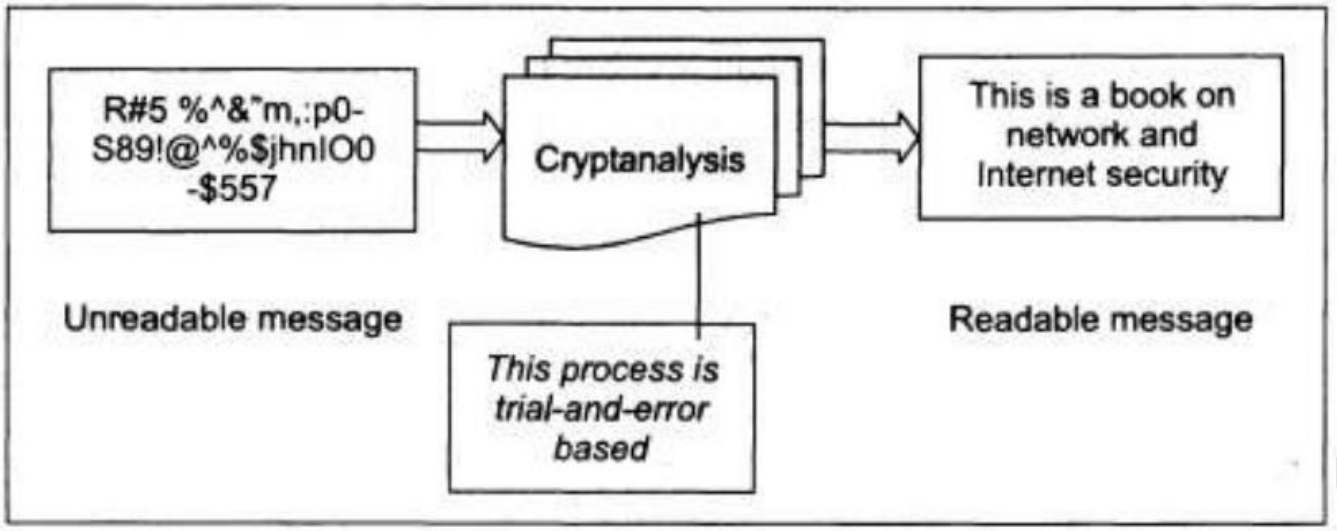
- Cryptography is the science of providing security for information.
- Process or Practice of the enciphering and deciphering of messages in secret code.
- It has been used to obtain secure communication between individuals, government agencies, banking, and military forces.
- The principles of cryptography are today applied to the encryption of FAX, TELEVISION and computer Network communications



Cryptographic system

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Cryptanalysis
is the technique of decoding messages from a non-redable format back to a readable format without knowing how they were initially converted from readable format to non-readable format.

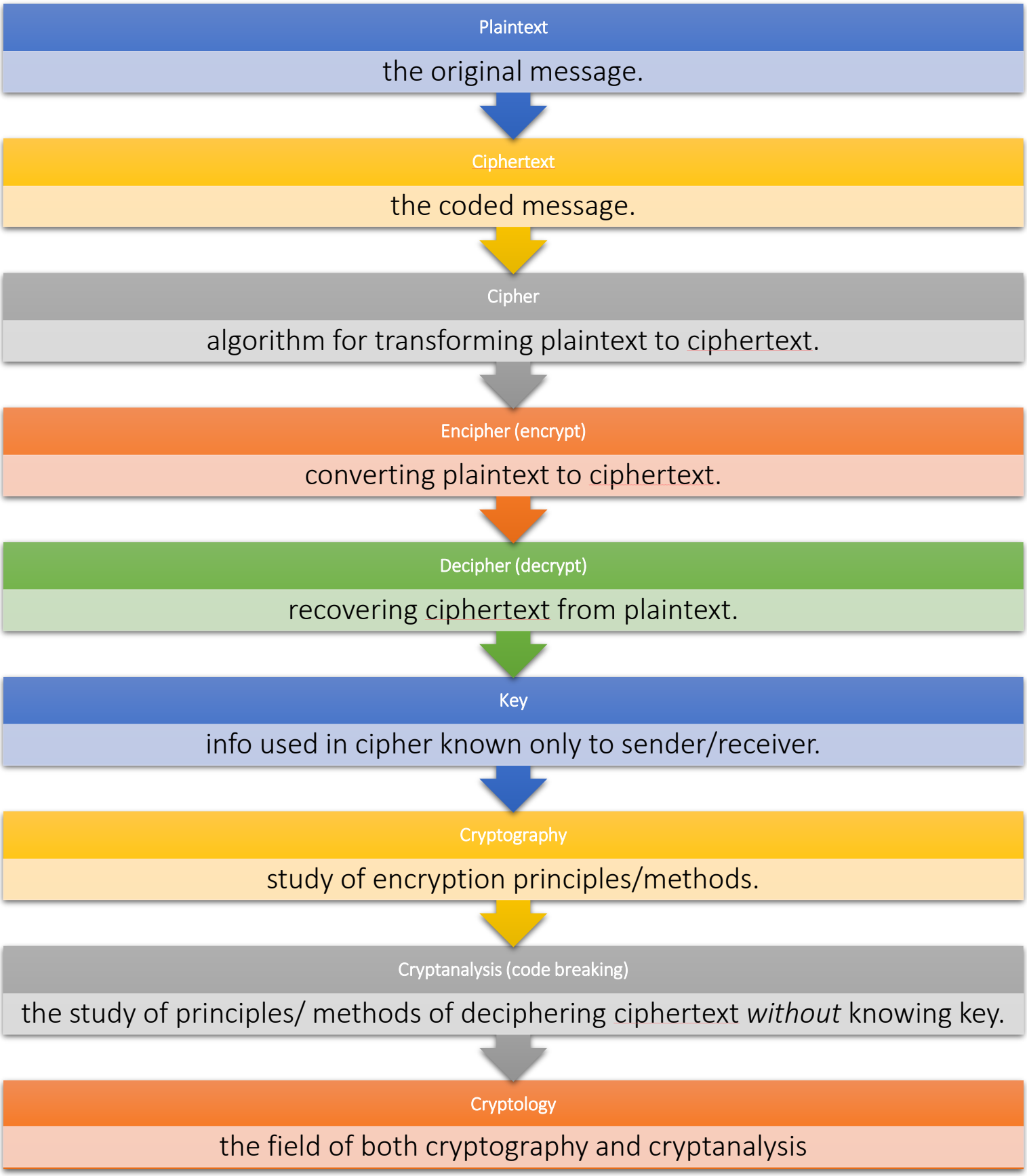


Cryptanalysis

Cryptology is a combination of cryptography and cryptanalysis.

❖ Basic Concepts (terminology)

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

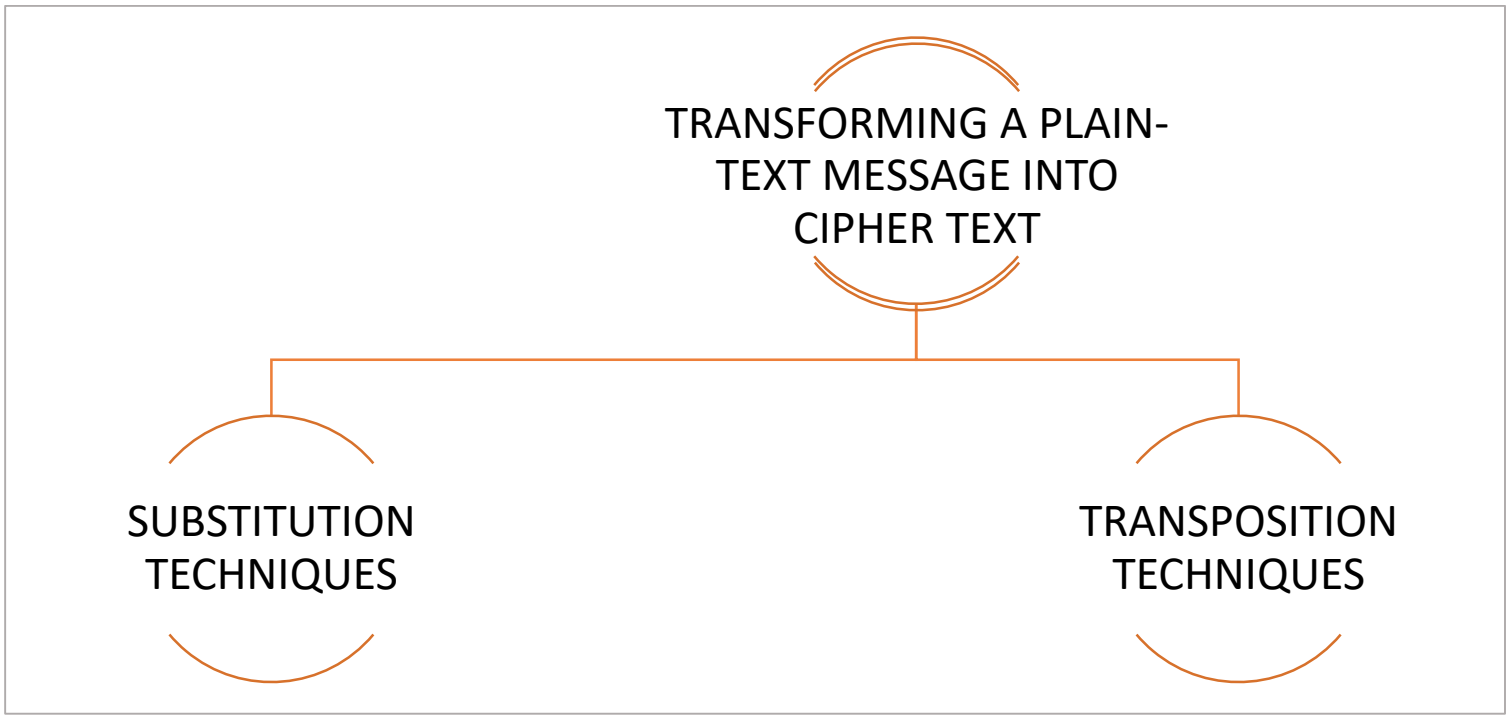


Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

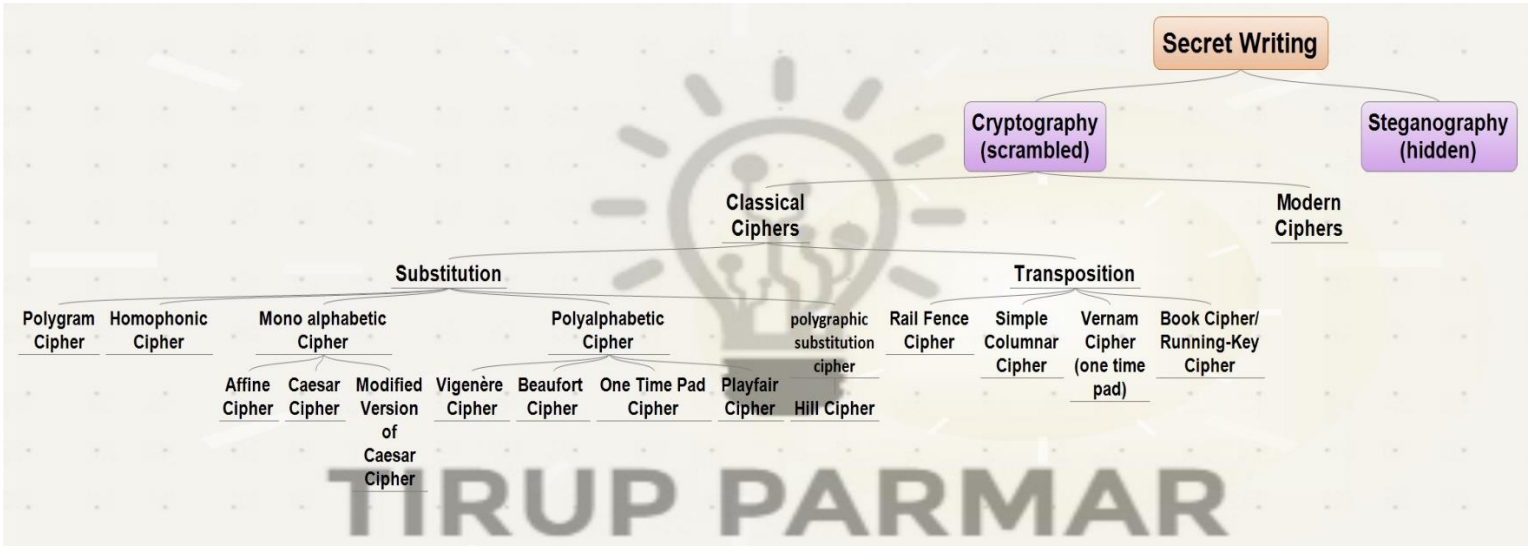
PLAIN TEXT AND CIPHER TEXT

Clear text, or **plain text**, signifies a message that can be understood by the sender, the recipient, and also by anyone else who gets access to that message.

There are two primary ways in which a plain-text message can be codified to obtain the corresponding cipher text: substitution and transposition.



Techniques for transforming plain text to cipher text



Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

❖ Cipher

In Cryptography, a cipher is an algorithm for performing encryption or decryption. It can be Symmetric or Asymmetric "a way of changing a message to keep it secret".

- Symmetric (Private-key cryptography): In Symmetric Key Algorithms same key used for encryption and decryption.
- Asymmetric (Public-key cryptography): In Asymmetric Key Algorithms different keys used for encryption and decryption.
  - Stream ciphers encrypt the digits (typically bits) of a message one at a time.
  - Block ciphers take a number of bits and encrypt them as a single unit (Block), Blocks of 64 or 128 bits have been commonly used.
- There are two types of ciphers:
  - Classical Ciphers
  - Modern Ciphers

1. Classical Ciphers

A classical cipher is a type of cipher that was used historically. In general, classical ciphers operate on an alphabet of letters (such as "A-Z"), and are implemented by hand or with simple mechanical devices.

- Sender and Recipient share a same key.
- All classical encryption & decryption algorithms are Symmetric.

Classical Cipher Types:

- Substitution Cipher
- Transposition Cipher

Substitution Cipher

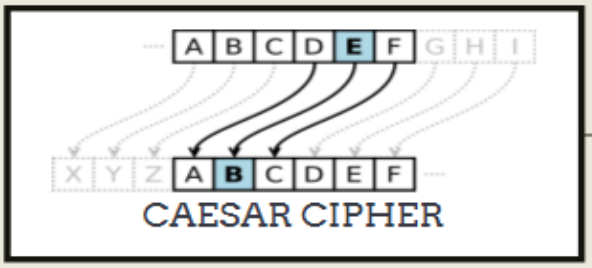
Is a method of encryption by which units of plaintext are replaced with Ciphertext, according to a regular systems.

Substitution Cipher Types

1- Monoalphabetic Cipher
2- Polyalphabetic Cipher
3- Polygram Cipher.
4- Homophonic Cipher.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

SUBSTITUTION TECHNIQUES

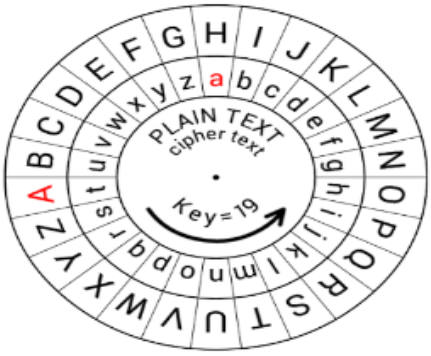


In the substitution-cipher technique, the characters of a plain-text message are replaced by other characters, numbers or symbols.

1. The scheme explained earlier (of replacing an alphabet with the one three places down the order) was first proposed by Julius Caesar, and is termed Caesar cipher.
2. It was the first example of substitution cipher. In the substitution-cipher technique, the characters of a plain-text message are replaced by other characters, numbers or symbols.
3. The Caesar cipher is a special case of substitution technique wherein each alphabet in a message is replaced by an alphabet three places down the line.
4. For instance, using the Caesar cipher, the plain-text ATUL will become cipher-text DWXO.
5. The Caesar cipher is a very weak scheme of hiding plain-text messages. All that is required to break the Caesar cipher is to do the reverse of the Caesar cipher process

i.e. replace each alphabet in a cipher-text message produced by Caesar cipher with the alphabet that is three places up the line.

6. Thus, to work backwards, take a cipher text produced by Caesar cipher, and replace each A with X, B with Y, C with Z, D with A, E with B and so on.



MODIFIED VERSION OF CAESAR CIPHER

THE CAESAR CIPHER IS GOOD IN THEORY, BUT NOT SO GOOD IN PRACTICE.

LET US NOW TRY AND COMPLICATE THE CAESAR CIPHER TO MAKE AN ATTACKER'S TASK DIFFICULT.

HOW CAN WE GENERALIZE CAESAR CIPHER A BIT MORE?

LET US ASSUME THAT THE CIPHER-TEXT ALPHABETS CORRESPONDING TO THE ORIGINAL PLAIN-TEXT ALPHABETS MAY NOT NECESSARILY BE THREE PLACES DOWN THE ORDER, BUT INSTEAD, CAN BE ANY PLACES DOWN THE ORDER. THIS CAN COMPLICATE MATTERS A BIT.

THUS, WE ARE NOW SAYING THAT AN ALPHABET A IN PLAIN TEXT WOULD NOT NECESSARILY BE REPLACED BY D.

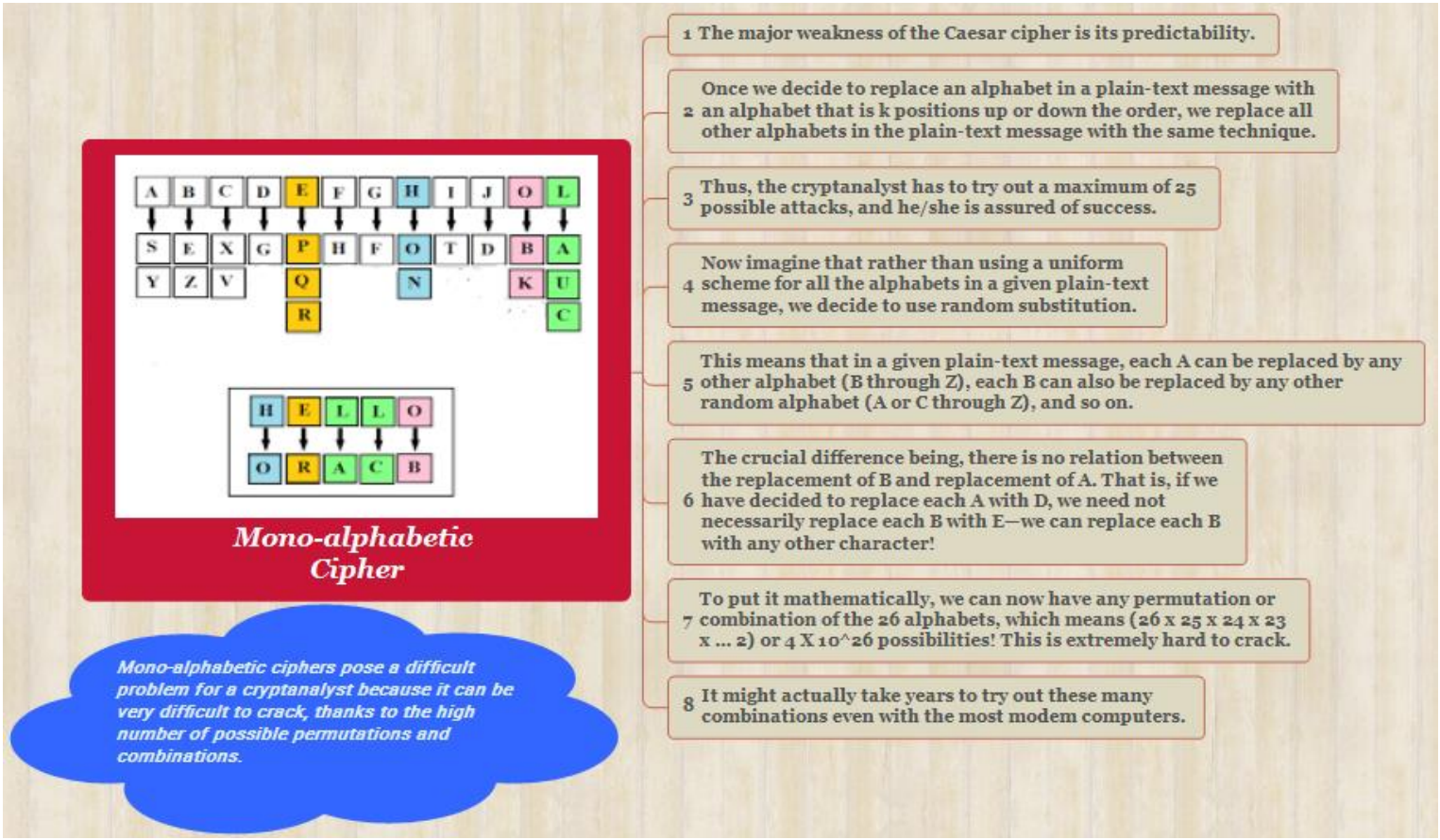
IT CAN BE REPLACED BY ANY VALID ALPHABET, I.E. BY E OR BY F OR BY G, AND SO ON.

ONCE THE REPLACEMENT SCHEME IS DECIDED, IT WOULD BE CONSTANT AND WILL BE USED FOR ALL OTHER ALPHABETS IN THAT MESSAGE.

AS WE KNOW, THE ENGLISH LANGUAGE CONTAINS 26 ALPHABETS. THUS, AN ALPHABET A CAN BE REPLACED BY ANY OTHER ALPHABET IN THE ENGLISH ALPHABET SET, (I.E. B THROUGH Z).

OF COURSE, IT DOES NOT MAKE SENSE TO REPLACE AN ALPHABET BY ITSELF (I.E. REPLACING A WITH A). THUS, FOR EACH ALPHABET, WE HAVE 25 POSSIBILITIES OF REPLACEMENT. HENCE, TO BREAK A MESSAGE IN THE MODIFIED VERSION OF CAESAR CIPHER, OUR EARLIER ALGORITHM WOULD NOT WORK.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar



Homophonic Cipher

In this cipher technique, , plaintext letters map to more than one cipher text symbol. Usually, the highest-frequency plaintext symbols are given more equivalents than lower frequency letters. In this way, the frequency distribution is flattened, making analysis more difficult.

- Since more than 26 characters will be required in the cipher text alphabet, various solutions are employed to invent larger alphabets such as a numeric substitution, uppercase, lowercase, upside down, and fanciful symbols etc.
- A Mantua Homophonic Cipher (15th century, Roman Empire) is an example to this type of cipher.

Example:

Plaintext: HE EATS THEN SLEEPS AND DREAMS **Ciphertext:** ??

Key: The following table is the key.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

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
11	21	89	58	QP	15	JK	55	BC	B	47	PB	AA	49	50	ZS	A	43	JK	J	90	76	CT	93	30	13
AZ	12	ZA	ND	69	RF	FR	OG	61	71	GC	VC	CG	BB	49	SC	SP	CR	87	77	QQ	VM	59	HR	XT	NE
@			47	??			81											XX	WO						
QA				99			SS											88							
XF				101																					
				DD																					
				YD																					

Homophonic Cipher Table

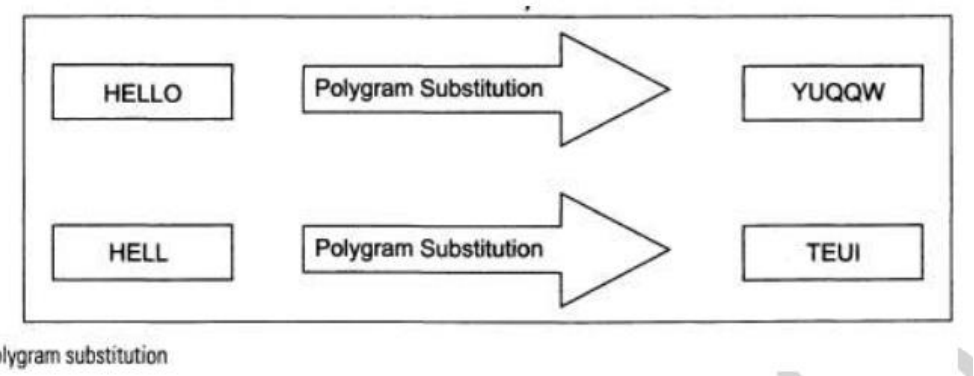
Ciphertext:

55QP69 **11JJK** 77OG?? **4987PB** 99101ZS **XXAZBB** 58ND43 **DD@AA** 88

Polygram Cipher

This cipher technique, replaces one block of plain text with a block of cipher text, it does not work on a character by character basis. This cryptosystem make cryptanalysis harder by destroying the single character frequencies.

- **Example:**
  - **HELLO HELL** Could be replaced by " YUQQW TEUI ".
  - **CAUSE OF BECAUSE** Could be replaced by " XAYWQOA MH IGAYK "
  - Despite the characters of the four blocks of text being almost the same.



Polygram substitution

- **Problems in PolyGram Substitution:**

Different keys are required for each block of characters. The encryption and decryption technique is applied to each and every block of character of a text differently: even when the block is repeated in the plain text. So it requires more time for encryption.

Polyalphabetic Cipher

Leon Battista invented the Polyalphabetic Substitution Cipher in year 1568. "Poly means Many in Greek language". This method uses a mixed alphabet to encrypt a message. These were thought to be unbreakable for almost 300 years.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

- The Enigma machine is more complex but still fundamentally a polyalphabetic substitution cipher.

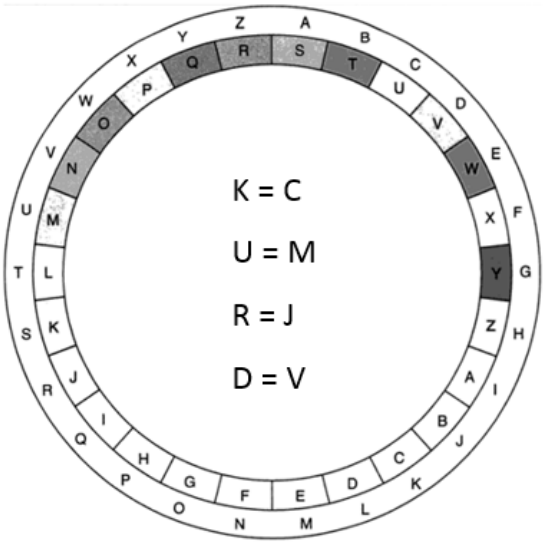
Polyalphabetic Cipher Types

A. Vigenère Cipher
B. Beaufort Cipher
C. One Time Pad Cipher
D. Playfair Cipher

A. Vigenère Cipher (Using Code Wheel)

A tool that was used for the Vigenère Cipher was a code wheel. The outer ring of the wheel represented plaintext letters and the inner wheel represented Ciphertext letters.

- **Encryption Method**: Go to the plaintext letter in the outer wheel and find its corresponding Ciphertext letter.
- **Encryption Method:** Position the keyword letter under "A" but go from the inner Ciphertext wheel to the outer plaintext wheel.



- **Example:**

Plain Text: KURD
Key = S
Cipher Text: CMJV
Decrypt this; " DGNW " **Key =** S & Use Code Wheel

- **Example1:**

Plain Text: " on a plane the plane is due " **Key =** milk
Cipher Text: ?

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

- Encode plain text.
- Write key under coded plaintext, repeating as many times as necessary.
- Encode key.
- Add key character code to corresponding plain text code (mod 26).
- Decoding of resulting integer is Ciphertext.
- Note: If (Pencoding + Kencoding) >= 26 then - 26

▪ **Example1:** Answer ▪ Note: If (Pencoding + Kencoding) >= 26 then - 26

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text	o	n	a	p	l	a	n	e	t	h	e	p	l	a	n	e	i	s	d	u	e				
Pencoding	14	13	0	15	11	0	13	4	19	7	4	15	11	0	13	4	8	18	3	20	4				
+ Key	m	i	l	k	m	i	l	k	m	i	l	k	m	i	l	k	m	i	l	k	m				
Kencoding	12	8	11	10	12	8	11	10	12	8	11	10	12	8	11	10	12	8	11	10	12				
Cipher Code	0	21	11	25	23	8	24	14	5	15	15	25	23	8	24	14	20	0	14	4	16				
Cipher Text	a	v	l	z	x	i	y	o	f	p	p	z	x	i	y	o	u	a	o	e	q				

▪ **Example2:** **Ciphertext:** " avlzxiyofppzxiyouaoep " **Key =** milk **Plaintext:** ?

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher Text	a	v	l	z	x	i	y	o	f	p	p	z	x	i	y	o	u	a	o	e	q				
Cipher Code	0	21	11	25	23	8	24	14	5	15	15	25	23	8	24	14	20	0	14	4	16				
– Key	m	i	l	k	m	i	l	k	m	i	l	k	m	i	l	k	m	i	l	k	m				
Kencoding	12	8	11	10	12	8	11	10	12	8	11	10	12	8	11	10	12	8	11	10	12				
Pencoding	14	13	0	15	11	0	13	4	19	7	4	15	11	0	13	4	8	18	3	20	4				
Plain Text	o	n	a	p	l	a	n	e	t	h	e	p	l	a	n	e	i	s	d	u	e				

0 – 12 = – 12 **26 – 12 = 14**

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Difficulty of Vigenère cipher

- The longer the keyword, the more difficult it will be for a third person to crack it.
- In fact, for any plain text and any cipher text of the same length, there is a key that connects them.

- **Example:**
  - consider the plain text: " enter plain text here "
  - The key connecting them (ignoring spaces) is: " arlanptewrlahlxan "
  - The cipher text will be: " eeeee eeeee eeee eeee "

B. Beaufort Cipher

The Beaufort cipher, created by Sir Francis Beaufort, The Beaufort cipher is a Reciprocal Cipher that is, Encryption and Decryption algorithms are the same.

Encryption & Decryption Methods:

- Firstly, choose the plaintext character from the top row of the tableau, call this column P.
- Secondly, travel down column P to the corresponding keyLetter K.
- Finally, move directly left from the Key letter to the left edge of the tableau, the Ciphertext encryption of Plaintext P with Key K will be there.

- **Example:** **Plaintext:** " HOW STUFF WORKS '' **Key =** CIPHER
- **Example: Answer**

Plain	H	O	W	S	T	U	F	F	W	O	R	K	S
Key	C	I	P	H	E	R	C	I	P	H	E	R	C
Cipher	J	W	L	Z	X	L	H	N	L	V	V	B	U

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

C. One Time Pad Cipher

known as Vernam Cipher is implemented using a random set of non repeating characters as the Key. The rest of process is same as the Vigenère cipher.

Example1: **Plaintext:** " HOW ARE YOU '' **Key =** NCBTZQARX **Ciphertext:** ?

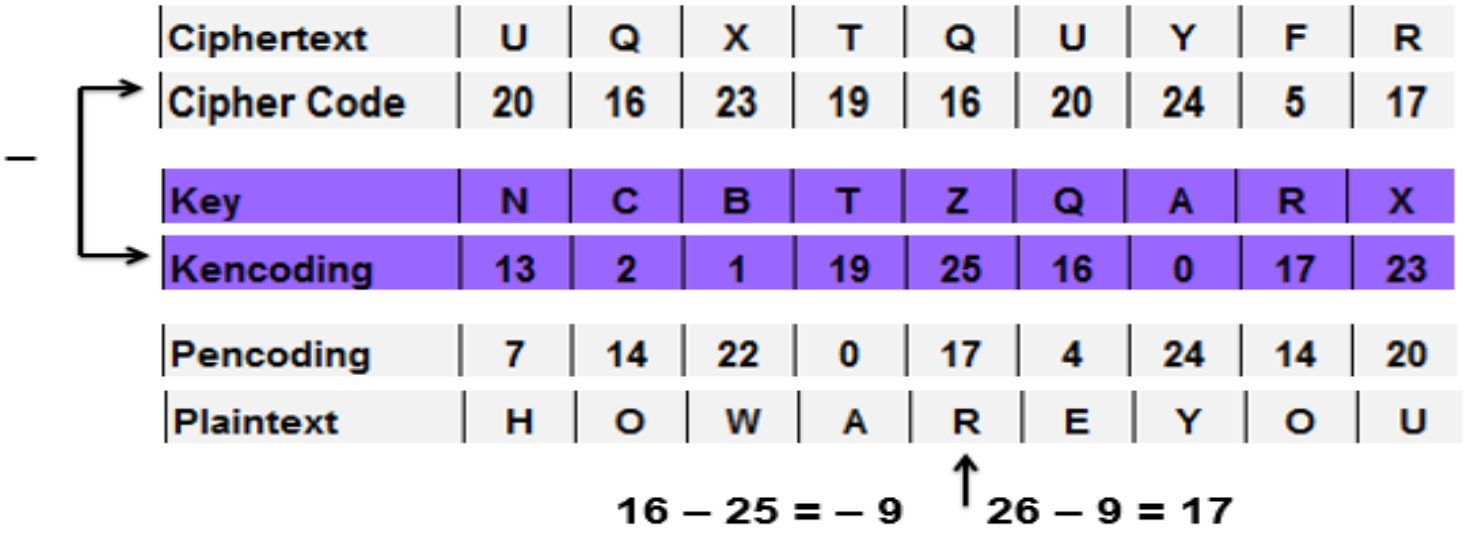
- *Note: If (Pencoding + Kencoding) >= 26 then - 26*

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
1	2	**3**	4	**5**	6	**7**	8	**9**	10	**11**	12	**13**	14	**15**	16	**17**	18	**19**	20	**21**	22	**23**	24	**25**	26

	Plaintext	H	O	W	A	R	E	Y	O	U
	Pencoding	7	14	22	0	17	4	24	14	20
+	Key	N	C	B	T	Z	Q	A	R	X
	Kencoding	13	2	1	19	25	16	0	17	23
	Cipher Code	20	16	23	19	16	20	24	5	17
	Ciphertext	U	Q	X	T	Q	U	Y	F	R

Example2: **Ciphertext:** " UQXTQUYFR '' **Key =** NCBTZQARX **Plaintext:** ?

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar



D. Playfair Cipher

The Playfair cipher encrypts pairs of letters, instead of single letters. This is significantly harder to break. Each plaintext letter is replaced by a diagram in this cipher.

- User chooses a keyword and puts it in the cells of a 5 x 5 matrix.
- Letter I and J always stay in one cell .
- Duplicate letters appear only once.
- Number of diagrams is 26 x 26 = 676.

Playfair Cipher Rules

- Group plaintext letters two at a time.
- Separate repeating letters with an x.
- Plaintext letters in the same row are replaced by letters to the right.
- Plaintext letters in the same column are replaced by letters below.
- Plaintext letters in different row and column are replaced by the letter in the row corresponding to the column of the other letter and vice versa.

- **Example1: Plaintext:** CRYPTO IS TOO EASY **Key =** INFOSEC **Ciphertext:** ??
  Grouped text: CR YP TO IS TO XO EA SY
  Ciphertext: AQ TV YB NI YB YF CB OZ

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

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

- **Example2: Ciphertext:** AQTVYBNIYBYFCBOZ **Key =** INFOSEC **Plaintext:** ??
  Grouped text: AQ TV YB NI YB YF CB OZ
  Plaintext: CR YP TO IS TO XO EA SY

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

- **To Decrypt:** The receiver reconstructs the 5 x 5 matrix using the keyword and then uses the same rules as for encryption.

Hill Cipher

The **Hill cipher** works on multiple letters at the same time. Hence, it is a type of polygraphic substitution cipher. Lester Hill invented this in 1929. The Hill cipher has its roots in the matrix theory of mathematics. More specifically, we need to know how to compute the inverse of a matrix.

WORKING

- Treat each letter with a number like A=0, B=1, C=2……
- Let us say, our original message is "TAJ"
- As per the rule, T=19 A=0 J=9
- Convert into matrix form as

$$\begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix}$$

- Now ***multiply the plain text matrix with any number as keys***. The multiplying matrix should be of *n* x *n* where n is the number of rows of original matrix

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times \begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix}$$

- Now compute ***mod 26*** on resultant matrix i.e. take the remainder after dividing by 26.

$$\begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 25 \\ 21 \end{bmatrix}$$

- Now translating numbers into alphabets, we get:

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

19=T 25= Z 21=V

- Therefore, our cipher text is ***TZV***

To decrypt hill cipher, follow the steps:

1.) take cipher text matrix and multiply it by inverse of original key matrix
2.) Again perform mod by 26.
Thus we get our original text.

Transposition techniques

1. Rail Fence Cipher

The Rail Fence Cipher involves writing messages so that alternate letters are written on separate upper and lower lines. The security of the cipher can be improved by choosing more than two lines to encrypt your message with.

- **Example1: Rail fence of depth 2**
- To encrypt, write the plaintext in a zigzag pattern in two rows and form the cipher text by reading off the letters from the first row followed by the second.
- To decrypt, write the cipher text in two rows and read off the plaintext in a zigzag fashion.

Plain text: meet me after the toga party

Row 1: m e m a t r h t g p r y

Row 2: e t e f e t e o a a t

Cipher text: m e m a t r h t g p r y e t e f e t e o a a t

- **Example2: Rail fence of depth 3**

Plain text: meet me after the toga party

Row 1: m m t h g r

Row 2: e t e f e t e o a a t

Row 3: e a r t p y

Cipher Text: MMTHGRETEFETEOAATEARTPY

Decrypt this: " IOEUDSALVKRITN **"** **Key:** Rail fence of depth 3

Decrypt this: " IWTKGAAAEHNSOOMKATD **"** **Key:** Rail fence of depth 3

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Simple Columnar Transposition Technique:

A columnar transposition, also known as a row-column transpose, is a very simple cipher to perform by hand. First, you write your message in columns. Then, you just rearrange the columns. For example. I have the message, "Which wristwatches are swiss wristwatches." You convert everything to upper case and write it without spaces. When you write it down, make sure to put it into columns and number them. Let's use five columns.

	Unencoded	Rearranged
Column #:	4 2 5 3 1	1 2 3 4 5
	W H I C H	H H C W I
	W R I S T	T R S W I
	W A T C H	H A C W T
	E S A R E	E S R E A
	S W I S S	S W S S I
	W R I S T	T R S W I
	W A T C H	H A C W T
	E S	S E

Now, you just read the columns down in the order that you number them. Above, you will see the key is 4 2 5 3 1, which means you write down the last column first, then the second, then the fourth, the first, and finally the middle. When you are all done, you will get "HTHESTHHRASWRASCSCRSSCWWWESWWEIITAIIT". I can put the example's information into the encoder for you: Encode or Decode

This columnar transposition cipher implementation will also move spaces around, so you can take "a b c" with a key of "2 1" and get " abc" (note the two spaces in front). I suggest you remove all spaces before you encode the text, but they should be preserved even if you don't. Newlines are ignored and not taken into consideration.

Vernam Cipher (one-time pad)

Vernam Cipher is also known as one-time pad and it is implemented using the random set of non-repeating characters as the input cipher text. The same cipher text is not used for any other text message. The algorithm steps are as follows:

Each plain text is given a number in an increasing sequence like A=0, B=1…Z=25
Same is repeated for each character in the cipher text
The plain text number and corresponding cipher text number are added. If the sum is greater than 26 then 26 is subtracted from the sum
Each resulting number is translated to its corresponding alphabet. That is the output cipher text.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Original Message: ATTACKTAJ

Plain text	A	T	T	A	C	K	T	A	J
	0	19	19	0	2	10	19	0	9
+									
One Time Pad (substitute with any letters which are used only ones)	N	B	D	E	P	S	F	Z	L
	13	1	3	4	15	18	5	25	11
Initial Total	13	20	22	4	17	28	24	25	20
Substract 26, If >25	13	20	22	4	17	2	24	25	20
Substitute	N	U	W	E	R	C	Y	Z	U

Book Cipher/Running-Key Cipher

- The idea used in **book cipher,** also incorrectly called **running-key cipher,** is quite simple, and is similar in principle to the Vernam cipher.
- For producing cipher text, some portion of text from a book is used, which serves the purpose of a one-time pad.
- Thus, the characters from a book are used as onetime pad, and they are *added* to the input plain-text message similar to the way a one-time pad works.

Encryption & Decryption

- Encryption or Encoding or Encode
  - The process of converting plain text into cipher text is called as encoding.
- Decryption or Decoding or Decode
  - The process of converting cipher text into plain text is called as decoding.

The important aspects of Encryption & Decryption process are:

- Algorithm
  - The technique/ method used to encrypt or decrypt. Algorithm is generally not kept

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

secret.

- Key
  - A key is a character or a group of characters used to encrypt or decrypt the plain text. A key is generally kept secret.

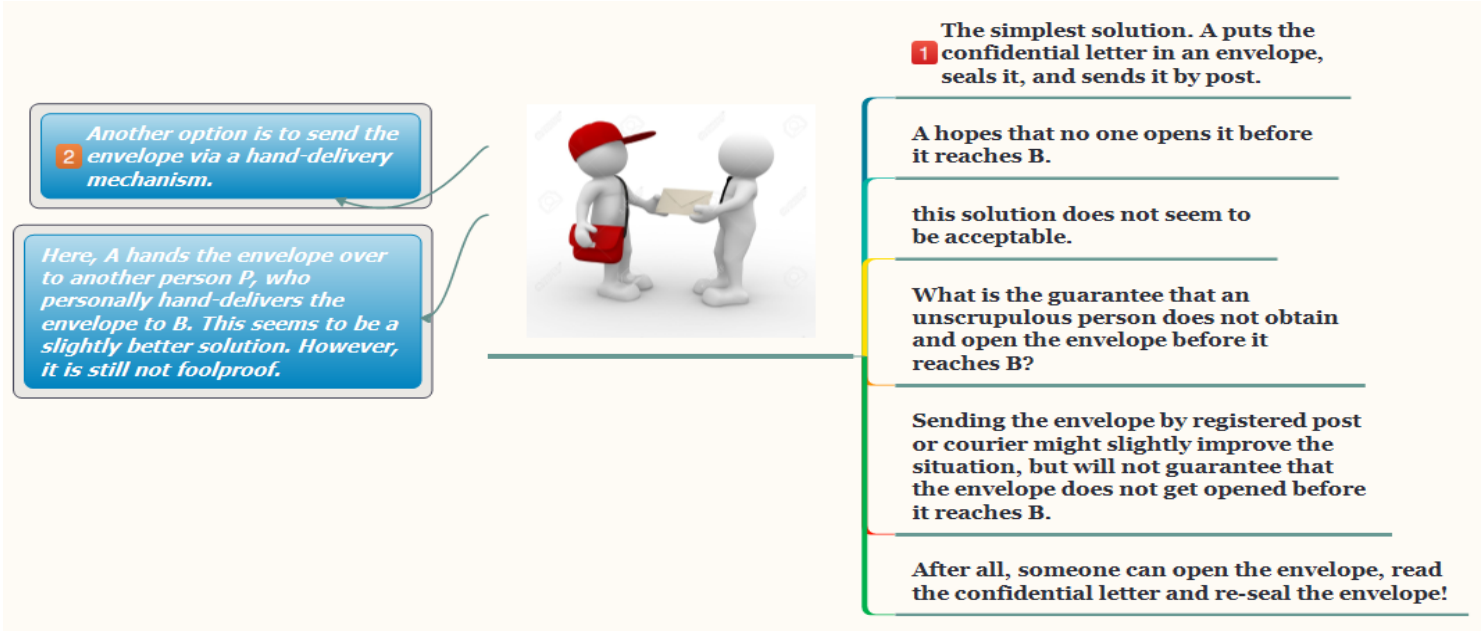
Depending on what keys are used, there are two types of cryptography mechanisms:-

- **Symmetric Key Cryptography**
  Symmetric key cryptography involves the usage o f the same key for encryption and decryption.
- **Asymmetric Key Cryptography**
  Asymmetric key cryptography involves the usage of one key for encryption, and another, different key for decryption.

Symmetric Key Cryptography and the Problem of Key Distribution

why we need two different types of cryptographic algorithms in the first place. To understand this, let us consider a simple problem statement.

Person A wants to send a highly confidential letter to another person B. A and B both reside in the same city, but are separated by a few miles, and for some reason, cannot meet each other.



This solution has not only prevented unauthorized access to the letter, but also the authorized access.

BOB COMES UP WITH ANOTHER IDEA

That is, even B would not be able to open the lock. This defeats the purpose of sending the letter in this manner, in the first place.

Bob now puts the envelope inside a box, seals that box with a highly secure lock, and sends the box to Alice (through the mechanism of post/courier/hand-delivery).

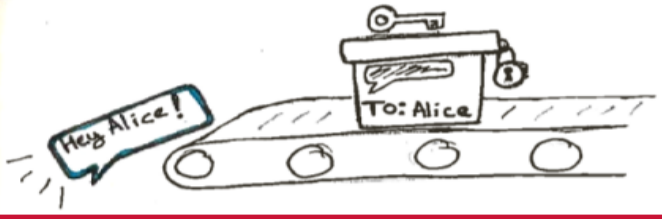
Since the lock is highly secure, nobody can open the box while in transit, and therefore, open the envelope.

Consequently, nobody will be able to read/ access the highly confidential letter!

The problem is resolved! If we think about it, we will realize that the problem indeed seems to be resolved.

However, this solution has given birth to a new problem.

How on earth can the intended recipient (Alice) now open the box, and therefore, the envelope?

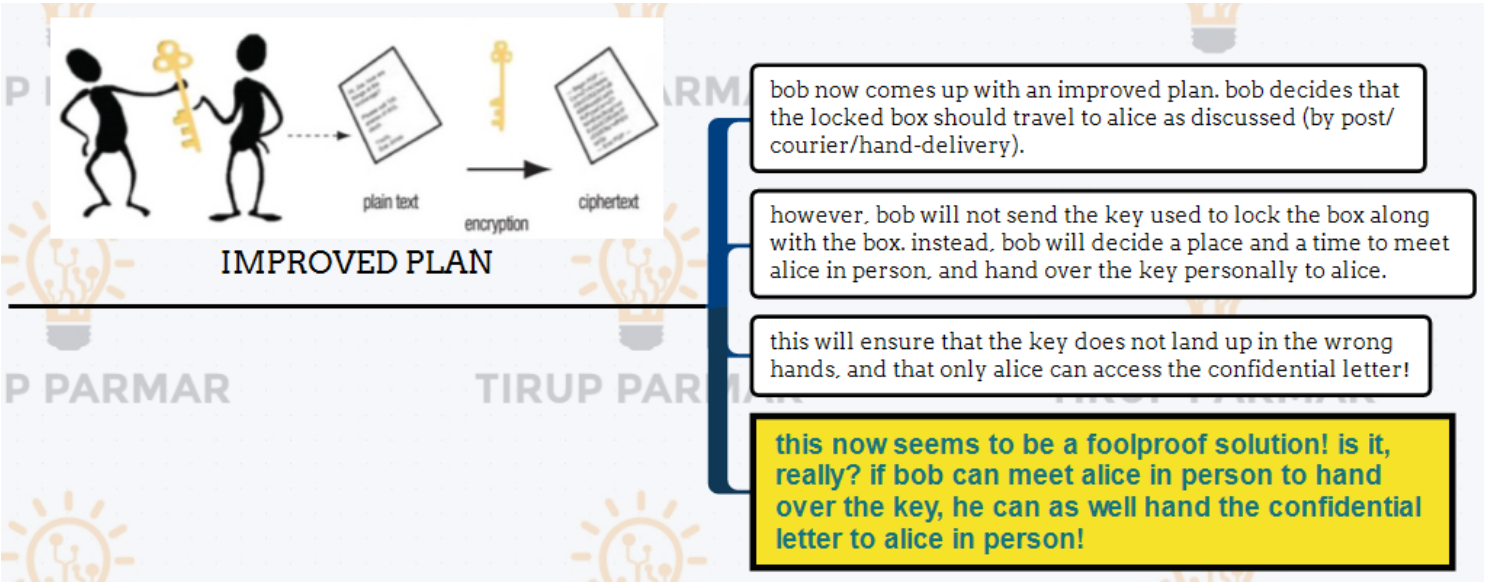


Another solution

What if Bob also sends the key of the lock along with the box, so that Alice can open the lock, and get access to the envelope inside the box, and hence the letter?

This seems absurd. If the key travels with the box, anybody who has access to the box in transit (e.g. Tom) can unlock and open the box.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar



Why have all these additional worries and overheads? Remember that the whole problem started because Alice and Bob
cannot, for some reason, meet in person!
As a result, we will observe that no solution is completely acceptable. Either it is not foolproof, or is not practically possible.
This is the problem of key distribution or key exchange.
Since the sender and the receiver will use the same key to lock and unlock, this is called *symmetric key operation* (when used in the context of cryptography, this operation is called symmetric key cryptography).
Thus, we observe that the key distribution problem is inherently linked with the symmetric key operation.

Let us now imagine that not only Alice and Bob but also thousands of people want to send such confidential letters securely to each other.
What would happen if they decide to go for symmetric key operation?
If we examine this approach more closely, we can see that it has one big drawback if the number of people that want to avail of its services is very large.

We will start with small numbers and then inspect this scheme for a larger number of participants.

- For instance, let us assume that A now wants to communicate with two persons, B and C, securely.
- Can A use the same kind of lock (i.e. a lock with the same properties, which can be opened with the same key) and key for sealing the box to be sent to B and C?
- Of course, this is not advisable at all! After all, if A uses the same kind of lock and key to seal the boxes addressed for B and C, what is the guarantee that B does not open the box intended for C, or vice versa (because B and C would also possess the same key as A)?
- Even if B and C live in the two extreme comers of the city, A cannot simply take such a chance!
- Therefore, no matter how secure the lock and key is, **A must use a *different* lock-and-key pair for B and C.**
- **This means that A must buy two *different* locks and the corresponding two keys (i.e. one key per lock).**

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Parties involved	Number of lock-and-key pairs required
2(A,B)	1 (A-B)
3 (A, B, C)	3 (A-B, A-C, B-C)
4 (A, B, C, D)	6 (A-B, A-C, A-D, B-C, B-D, C-D)
5 (A, B, C, D, E)	10 (A-B, A-C, A-D, A-E, B-C, B-D, B-E, C-D, C-E, D-E)

Therefore, can we see that, in general, for *n* persons, the number of lock-and-key pairs is *n * (n* - l)/2?
Now,

if we have about 1,000 persons in this scheme,
we will have 1000 * (1000 - l)/2 = 1000 * (999)/2 = 99,9000/2 = 499,500 lock-and-key pairs!

In symmetric key cryptography key sharing is a big issue due to sending key directly or indirectly will lead to leak of key to an hacker.

Implementing Diffie Helman Key Exchange Algorithm

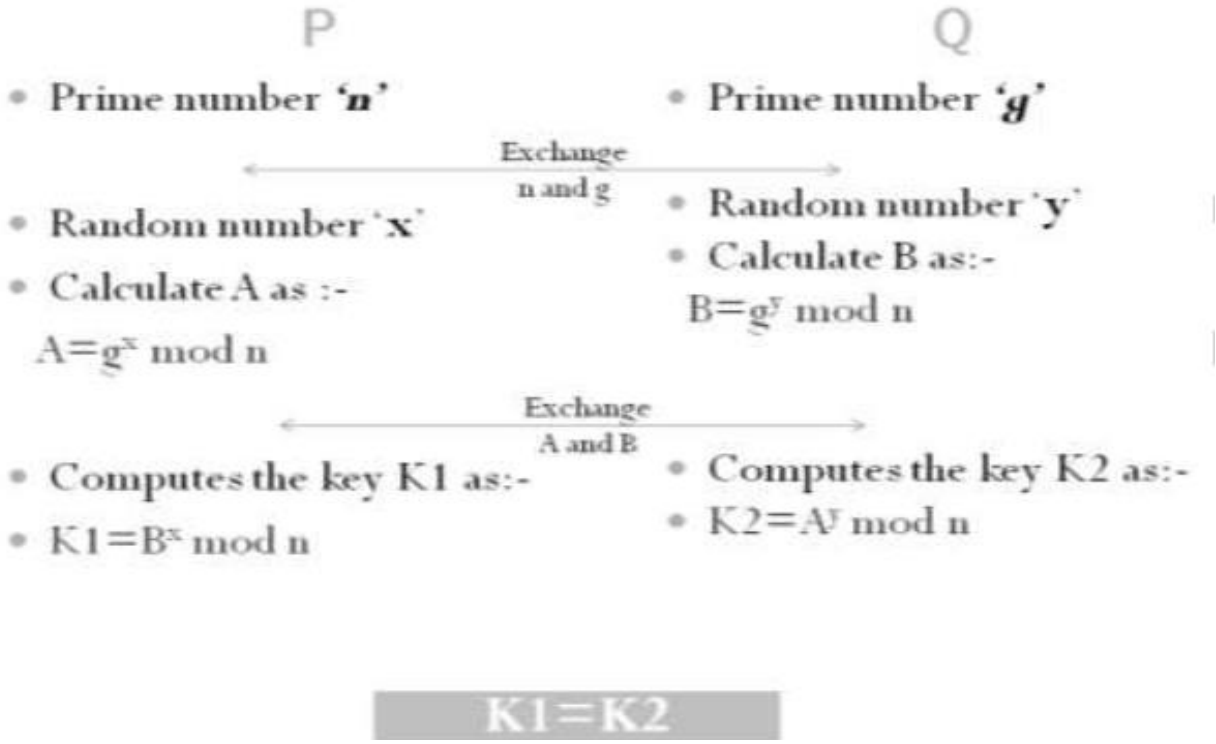
Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. The algorithm allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

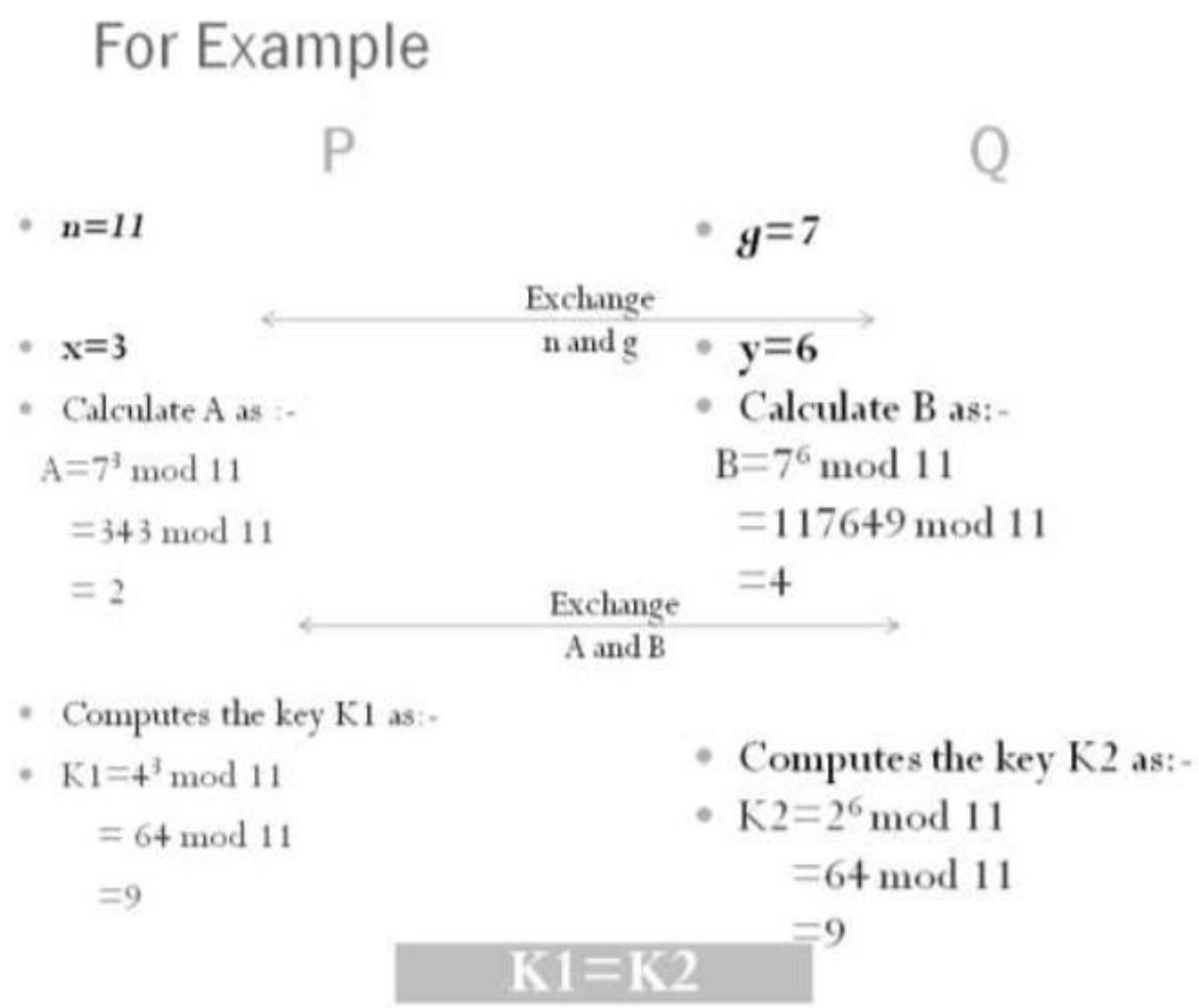
The algorithm can be briefly explained as below:

1. The two communicating parties A and B agree on two large primary numbers n and g. They are not a secret.
2. A internally selects another large random number ‘x’ and calculates a value V1 as $V1 = g^x \bmod n$
3. A sends V1 to B
4. B internally selects another large random number ‘y’ and calculates a value V2 as $V2 = g^y \bmod n$
5. B sends V2 to A
6. A computes secret key K1 as $K1=V2^x \bmod n$
7. B computes secret key K2 as $K2=V1^y \bmod n$

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Diffie-Hellman Key Exchange Algorithm





Problems with the Algorithm

Can we now consider that the Diffie-Hellman key-exchange algorithm solves all our problems associated with key exchange? Unfortunately, not quite!

The Diffie-Hellman key-exchange algorithm can fall pray to the **man-in-the-middle attack** (or to be politically correct, **woman-in-the-middle attack**), also called **bucket-brigade attack.**
The name *bucketbrigade attack* comes from the way firefighters of yesteryears formed a line between the fire and water source, and passed full buckets towards the fire and the empty buckets back.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

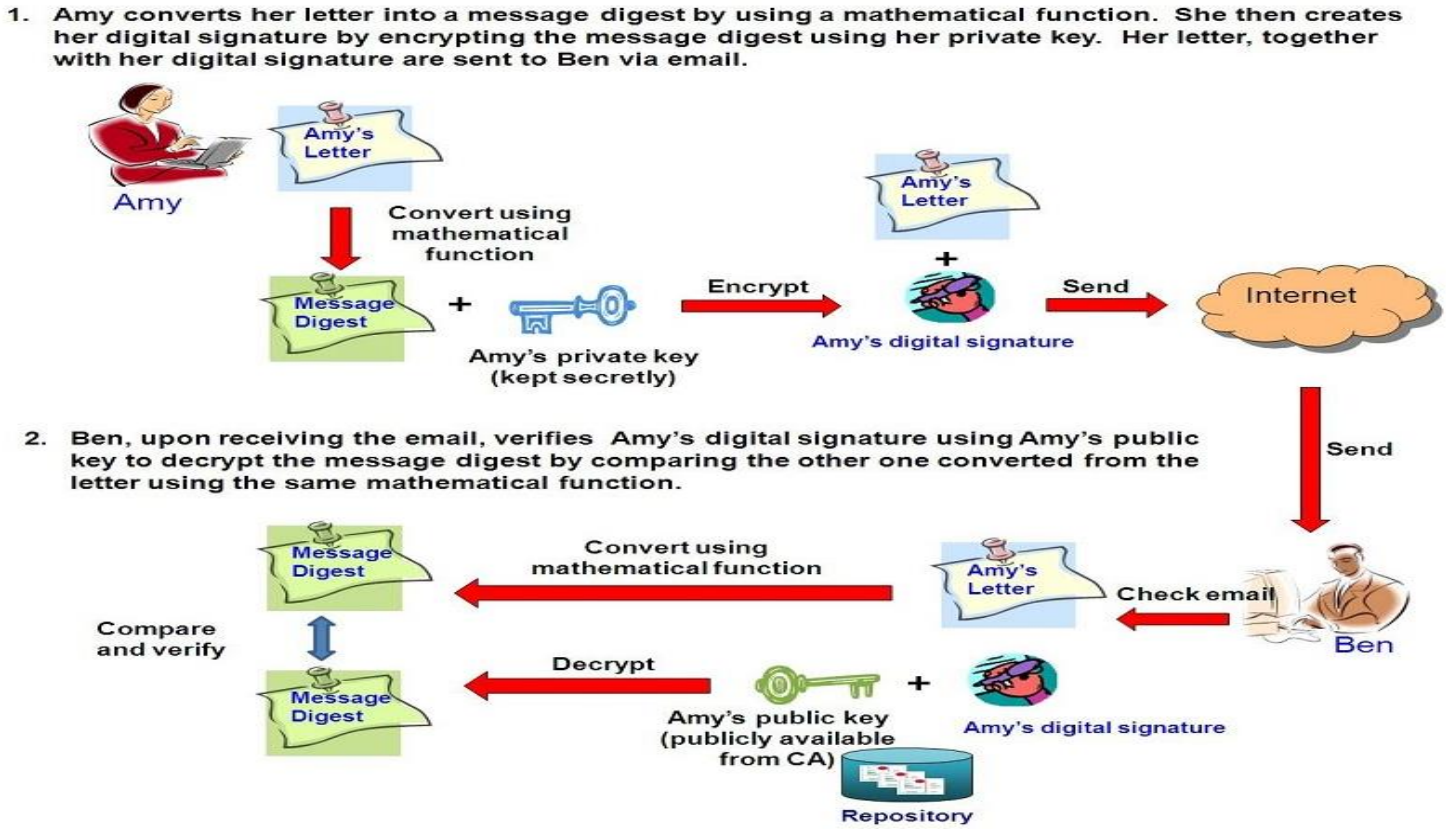
Alice		Tom		Bob	
$K1$	$= B^x \bmod n$	$K1$	$= B^x \bmod n$	$K2$	$= A^y \bmod n$
	$= 4^3 \bmod 11$		$= 8^8 \bmod 11$		$= 9^9 \bmod 11$
	$= 64 \bmod 11$		$= 16777216 \bmod 11$		$= 387420489 \bmod 11$
	$= 9$		$= 5$		$= 5$
		$K2$	$= A^y \bmod n$		
			$= 2^6 \bmod 11$		
			$= 64 \bmod 11$		
			$= 9$		

In this example Tom intercept in between and acts as a middle man, and sharing if keys is actually done between Alice and Tom and Bob and Tom.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Asymmetric Key Operation

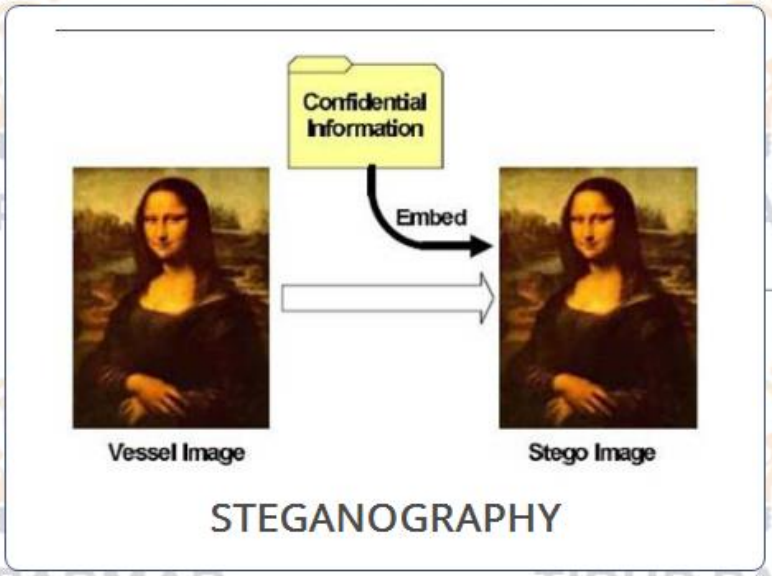
- Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic algorithms which require two separate keys, one of which is secret (or private) and one of which is public.
- Although different, the two parts of this key pair are mathematically linked.
- The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature.



Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

STEGANOGRAPHY

- Steganography is a technique that facilitates hiding of a message that is to be kept secret inside other messages.
- This results in the concealment of the secret message itself!
- Historically, the sender used methods such as invisible ink, tiny pin punctures on specific characters, minute variations between handwritten characters, pencil marks on handwritten characters, etc.



People hide secret messages within graphic images.

For instance, suppose that we have a secret message to send. We can take another image file and we can replace the last two rightmost bits of each byte of that image with (the next) two bits of our secret message.

The resulting image would not look too different, and yet carry a secret message inside!

The receiver would perform the opposite trick: it would read the last two bits of each byte of the image file, and reconstruct the secret message.

KEY RANGE AND KEY SIZE

The encrypted messages can be attacked, too! Here, the cryptanalyst is armed with the following information:

- The encryption/decryption algorithm
- The encrypted message
- Knowledge about the key size (e.g. the value of the key is a number between 0 and 100 billion)

the encryption/decryption algorithm is usually not a secret—everybody knows about it. Also, one can access an encrypted message by various means (such as by listening to the flow of information over a network). Thus, only the actual value of the key remains a challenge for the attacker. If the key is found, the attacker can resolve the mystery by working backwards to the original plain-text message.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

In order to protect ourselves against a brute-force attack, the key size should be such that the attacker cannot crack it within a specified amount of time.

- WORKS ON THE PRINCIPLE OF TRYING EVERY POSSIBLE KEY IN THE KEY RANGE, UNTIL YOU GET THE RIGHT KEY.
- IT USUALLY TAKES A VERY SMALL AMOUNT OF TIME TO TRY A KEY.
- THE ATTACKER CAN WRITE A COMPUTER PROGRAM THAT TRIES MANY SUCH KEYS IN ONE SECOND.
- IN THE BEST CASE, THE ATTACKER FINDS THE RIGHT KEY IN THE FIRST ATTEMPT ITSELF, AND IN THE WORST CASE, IT IS THE 100 BILLIONTH ATTEMPT.
- HOWEVER, THE USUAL OBSERVATION IS THAT THE KEY IS FOUND SOMEWHERE IN BETWEEN THE POSSIBLE RANGE.
- MATHEMATICS TELLS US THAT ON AN AVERAGE, THE KEY CAN BE FOUND AFTER ABOUT HALF OF THE POSSIBLE VALUES IN THE KEY RANGE ARE CHECKED. OF COURSE, THIS IS JUST A GUIDELINE, AND MAY OR MAY NOT WORK IN REAL PRACTICE FOR A GIVEN SITUATION.

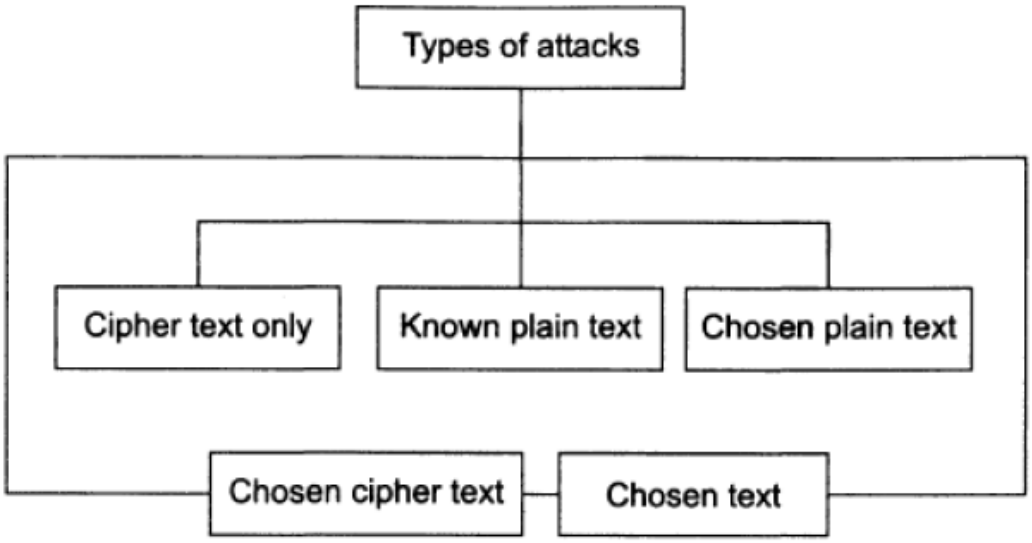
Efforts required to break a key

Key size on bits	Time required to search 1 percent of the key space	Time required to search 50 percent of the key space
66	1 second	1 minute
57	2 seconds	2 minutes
58	4 seconds	4 minutes
64	4.2 minutes	4.2 hours
72	17.9 hours	44.8 days
80	190.9 days	31.4 years
90	535 years	321 centuries
128	146 billion millennia	8 trillion millennia

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

POSSIBLE TYPES OF ATTACKS

Based on the discussion so far, when the sender of a message encrypts a plain-text message into its corresponding cipher text, there are five possibilities for an attack on this message



1. *Cipher-Text Only Attack*

- The attacker analyzes the cipher text at leisure to try and figure out the original plain text.
- Based on the frequency of letters (e.g. the alphabets e, i, a are very common in English, etc.) the attacker makes an attempt to guess the plain text.
- Obviously, the more cipher text available to the attacker, more are the chances of a successful attack.

2. *Known Plain-Text Attack*

- attacker knows about s()me pairs of plain text and corresponding cipher text for those pairs.
- Using this information, the attacker tries to find other pairs, and therefore, know more and more of the plain text.
- Examples of such *known plain texts* are company banners, file headers, etc., which are found commonly in all the documents of a particular company.
- How can the attacker obtain the plain text, in the first place? This can happen because plain-text information may become outdated over time, and hence, become public knowledge.

3. *Chosen Plain-Text Attack*

- the attacker selects a plain-text block, and tries to look for the encryption of the same in the cipher text.
- Here, the attacker is able to choose the messages to encrypt.
- Based on this, the attacker intentionally picks patterns of cipher text that result in obtaining more information about the key.

4. *Chosen Cipher-Text Attack*

- In the **chosen cipher-text attack,** the attacker knows the cipher text to be decrypted, the encryption algorithm that was used to produce this cipher text, and the corresponding plain-text block.
- The attacker's job is to discover the key used for encryption.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

- However, this type of attack is not very commonly used.

5. *Chosen-Text Attack*

- The **chosen-text attack** is essentially a combination of *chosen plain-text attack* and *chosen cipher text attack.*

Summary of types of attacks

Attack	Things known to the attacker	Things the attacker wants to find out
Cipher-text only	• Cipher text of several messages, all of which are encrypted with the same encryption key. • Algorithm used	• Plain text messages corresponding to these cipher text messages • Key used for encryption
Known cipher text	• Cipher text of several messages, all of which are encrypted with the same encryption key. • Plain text messages corresponding to above cipher text messages • Algorithm used	• Key used for encryption • Algorithm to decrypt cipher text with the same key
Chosen plain text	• Cipher text and associated plain text messages • Chooses the plain text to be encrypted	• Key used for encryption • Algorithm to decrypt cipher text with the same key
Chosen cipher text	• Cipher text of several messages to be decrypted • Corresponding plain text messages	• Key used for encryption
Chosen text	• Some of the above	• Some of the above

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

Types of criminal attacks:

Attack	*Description*
Fraud	Modern fraud attacks concentrate on manipulating some aspects of electronic currency, credit cards, electronic stock certificates, checks, letters of credit, purchase orders, ATMs, etc.
Scams	Scams come in various forms, some of the most common ones being sale of services, auctions, multi-level marketing schemes, general merchandise and business opportunities, etc. People are enticed to send money in return of great profits, but end up losing their money. A very common example is the *Nigeria scam*, where an email from Nigeria (and other African countries) entices people to deposit money into a bank account with a promise of hefty gains. Whosoever gets caught in this scam loses money heavily.
Destruction	Some sort of grudge is the motive behind such attacks. For example, unhappy employees attack their own organization, whereas terrorists strike at much bigger levels. For example, in the year 2000, there was an attack against popular Internet sites such as Yahoo!, CNN, eBay, Buy.com, Amazon.com and e*Trade where authorized users of these sites failed to log in or access these sites.
Identity theft	This is best understood with a quote from Bruce Schneier: *Why steal from someone when you can just become that person?* In other words, an attacker does not steal anything from a legitimate user – he *becomes* that legitimate user! For example, it is much easier to manage to get the password of someone else's bank account or to actually be able to get a credit card on someone else's name. Then that privilege can be misused until it gets detected.
Intellectual property theft	Intellectual property theft ranges from stealing companies' trade secrets, databases, digital music and videos, electronic documents and books, software and so on.
Brand theft	It is quite easy to set up fake Web sites that look like real Web sites. How would a common user know if she is visiting the HDFC Bank site or an attacker's site? Innocent users end up providing their secrets and personal details on these fake sites to the attackers. The attackers use these details to then access the real site, causing an *identity theft*.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar

IP spoofing and IP sniffing:

Sniffing and Spoofing On the Internet, computers exchange messages with each other in the form of small blocks of data, called as packets. A packet, like a postal envelope contains the actual data to be sent and the addressing information. Attackers target these packets, as they travel from the source computer to the destination computer over the Internet. These attacks take two main forms: (a) **Packet sniffing** (also called as **snooping**) and (b) **Packet spoofing**. Since the protocol used in this communication is called as Internet Protocol (IP), other names for these two attacks are: (a) **IP sniffing** and (b) **IP spoofing**. The meaning remains the same.

Let us discuss these two attacks.

(a) **Packet sniffing**: Packet sniffing is a passive attack on an ongoing conversation. An attacker need not *hijack* a conversation, but instead, can simply observe (i.e. *sniff*) packets as they pass by. Clearly, to prevent an attacker from sniffing packets, the information that is passing needs to be protected in some ways. This can be done at two levels: (i) The data that is traveling can be encoded in some ways or (ii) The transmission link itself can be encoded. To read a packet, the attacker somehow needs to access it in the first place. The simplest way to do this is to control a computer via which the traffic goes through. Usually, this is a router. However, routers are highly protected resources. Therefore, an attacker might not be able to attack it and instead, attack a less-protected computer on the same path.

(b) **Packet spoofing**: In this technique, an attacker sends packets with a false source address. When this happens, the receiver (i.e. the party who receives these packets containing false address) would inadvertently send replies back to this forged address (called as **spoofed address**) and not to the attacker. This can lead to three possible cases:

- **(i) The attacker can intercept the reply** – If the attacker is between the destination and the forged source, the attacker can see the reply and use that information for *hijacking* attacks.
- **(ii) The attacker need not see the reply** – If the attacker's intention was a Denial Of Service (DOS) attack, the attacker need not bother about the reply.
- **(iii) The attacker does not want the reply** – The attacker could simply be *angry* with the host, so it may put that host's address as the forged source address and send the packet to the destination. The attacker does not want a reply from the destination, as it wants the host with the forged address to receive it and get confused.

Questions:

1. Explain vernam cipher with example. ***Or*** What is the principle behind One Time pads? Why is it highly secure?
2. List and explain types of criminal attacks.
3. Why there is need for security? Explain security models.
4. Explain IP spoofing and IP sniffing in detail.
5. Explain the concept of key range and key size.
6. Define the following terms: Cryptography, Cryptanalysis, Brute-force attack, Symmetric key Cryptography, Asymmetric key Cryptography,
7. What are transposition techniques? Explain any one with the help of an example.
8. What are the ethical and legal issues in computer security system?
9. Principles of security.
10. Types of active attacks. ***Or*** Explain the various ways of attack, such as known plain-text attack etc.?
11. Mono-alphabetic cipher.
12. Diffie-hellman Key exchange algorithm.
13. What are the two basic ways of transforming plain-text onto cipher-text?
14. Explain the principles of security.
15. Mono-alphabetic and Rail Fence Technique.

Query? Ping me on– tirup1488@gmail.com
Video lectures on - https://www.youtube.com/c/TirupParmar