UNIT-1 CLASSICAL ENCRYPTION TECHNIQUES

OBJECTIVE : The objective is to present an overview of the main concept of cryptography, understand the threats and attacks, understand ethical hacking.

CRYPTOGRAPHY —

Cryptography is the method of storing and transmitting data in a particular form so that only those for whom it is intended can read & process it. In greek, crypto refers to hidden secret and graphy refers to study.

IMPORTANT TERMS —

1. Plain Text : This is the original intelligible message that is fed into algorithm as input.
2. Cipher Text : This is the scrambled message produced as output depending on plain text and secret key.
3. Cipher : An algorithm for transforming an intelligible message into unintelligible message by either transposition or substitution techniques.
4. Secret key : Value independent of the plain text and of the algorithm.
5. Encryption algorithm : Performs various substitutions and transformations on the plain text.

6. Decryption algorithm : Takes the cipher text and secret key to produce original plain text.

7. Cryptanalysis : The study of principles and methods used to transform unintelligible message back into an intelligible message without knowledge of the key. It is also called as Code breaking.

8. Cryptanalyst : Person who breaks the cipher text without knowing the key.

9. Crypto System : A cryptosystem is a 5-tuple system consisting of (P, C, K, E, D) where

P – plaintext space

C – Ciphertext space

K – key space

E – encryption functions, $E_K : P \rightarrow C$

D – decryption functions, $D_K : C \rightarrow P$

Cryptosystem consists of 3 algorithms :

1. One for key generation
2. One for encryption
3. One for decryption.

COMPUTER SECURITY —

Also known as cyber security or IT security is the protection afforded to an automated information system inorder to attain the applicable objectives of preserving integrity, availability and confidentiality of info. system resources.

Network Security : Refers to prevention and monitoring unauthorized access, misuse of computer network & accessible resources.

Internet Security : To provide measures to protect data during their transmission over a collection of inter-connected networks.

Key Objectives of Computer Security :

1. Confidentiality – It consists of two concepts

   (a) Data Confidentiality : Assures that private or confidential information is not made available to unauthorized individuals.

   (b) Privacy : Assures that individuals control what info related to them may be collected and stored & by whom and to whom that info may be disclosed

2. Integrity – It consists of two concepts

   (a) Data Integrity : Assures that info and programs are changed only in specified & authorized manner.

   (b) System Integrity : Assures that a system performs its intended function in an impaired manner, free from unauthorized manipulation of the system.

3. Availability – Assures that systems work promptly and service is not denied to authorized users.

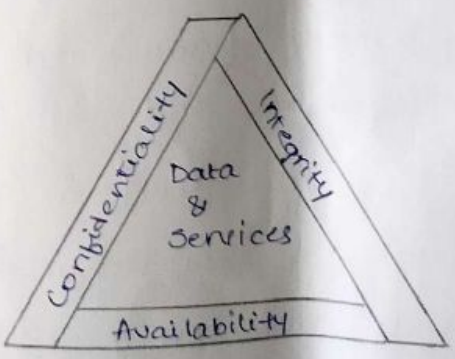
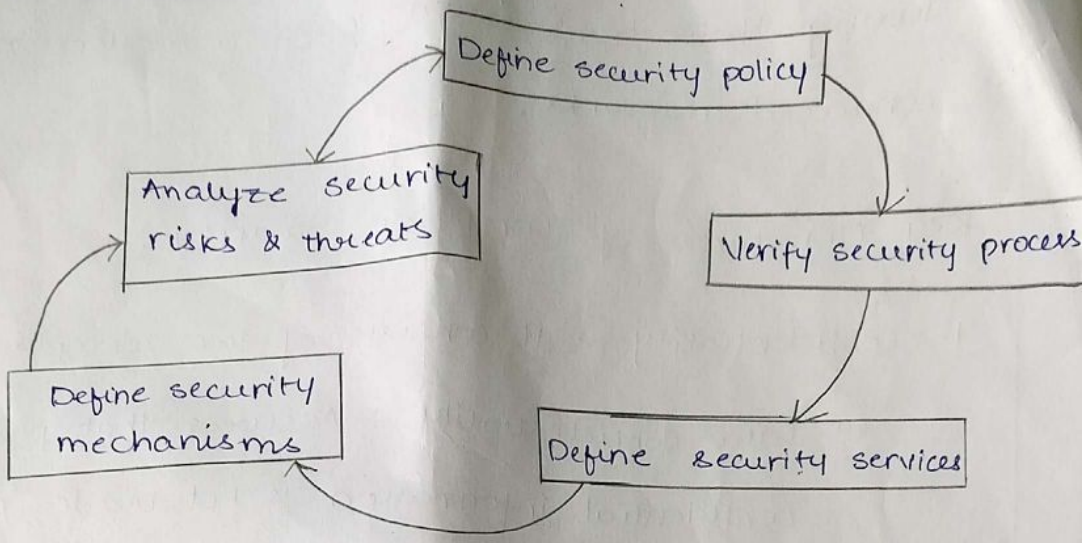


Fig : Security Requirements Triad.

SECURITY LIFECYCLE



1. Define security policy : Provides N/W security with the help of N/W tools and products.
2. Analyze risks and threats : To identify problems that are to be faced by the N/W.
3. Define security mechanisms : It detects, prevents and recover losses from threats
4. Define security services : Used to enhance security.
5. Verify security process : Checks the total process of security on the network.

OSI SECURITY ARCHITECTURE

Provides systematic framework for defining security attacks, mechanisms and services.

1. Security attacks are classified as either passive attacks which include unauthorized reading of a message of file and traffic analysis or active attacks such as modification of messages and denial of service.

2. A security mechanism is any process that is designed to detect, prevent or recover from a security attack.
3. Security services include authentication, access control, data confidentiality, data integrity, nonrepudiation and availability.

NOTE :

Threat is the possible danger that might exploit vulnerability.

Attack is an action taken against a target with the intention of doing harm.

Vulnerability is a weakness that makes targets susceptible to an attack.

SECURITY ATTACKS

An useful means of classifying security attacks, used in both X.800 and RFC 2828, is in terms of passive and active attacks. A passive attack attempts to learn or make use of info from the system but does not affect s/m resources. An active attack attempts to alter s/m resources.

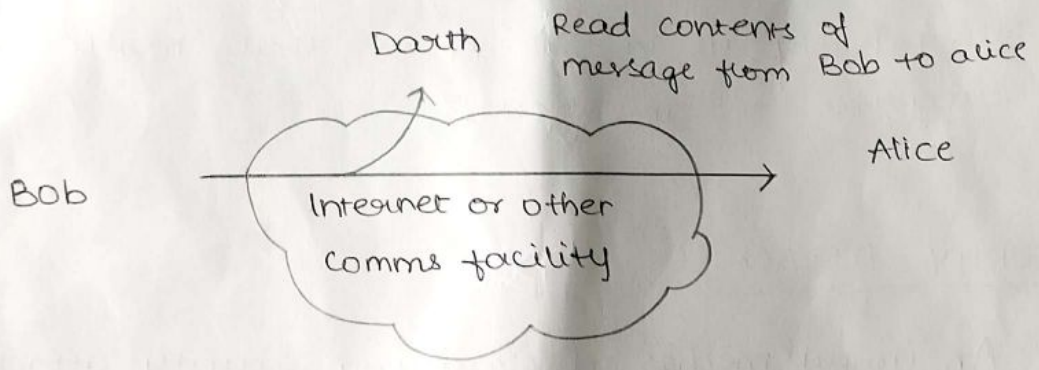
Passive Attack

The goal of the opponent is to obtain information that is being transmitted. The two types of passive attacks are: 1. Release of message contents — A telephone conversation, an e-mail, and any transfered file may contain sensitive or confidential info. To prevent an opponent

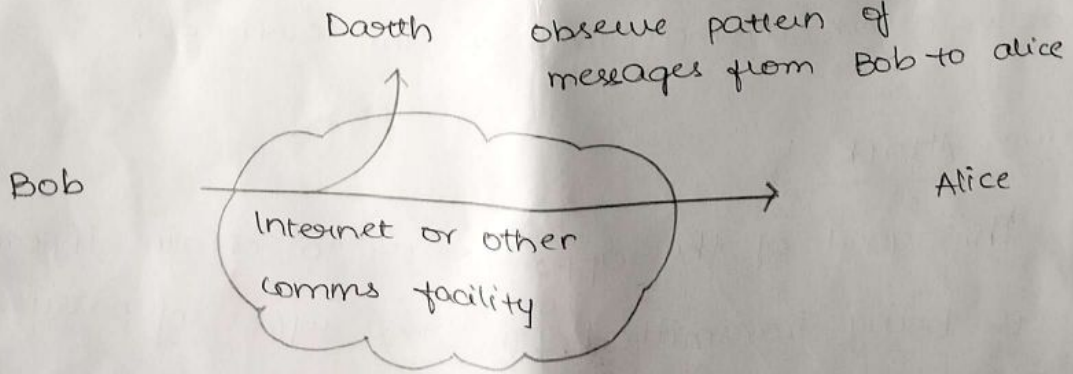
from learning the contents of these transmissions.

2. Traffic analysis — It is a way of masking the contents of message or other info traffic so that opponents, even if they captured the message, could not extract the info from message. The common technique for masking contents is encryption.

Passive attacks are very difficult to detect, because they do not involve any alteration of data. Typically, message traffic is sent and recieved normally and neither the sender nor reciever is aware that a third party has read the messages or observed the traffic pattern.



(a) Release of message contents



(b) Traffic analysis.

Active Attacks

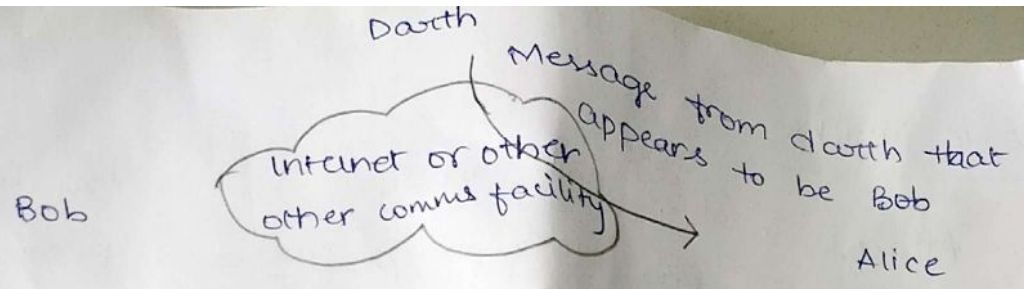
Attacks involve some modification of the data stream or the creation of a false stream and can be sub divided into 4 categories :

1. Masquerade : Takes place when one entity pretends to be a different entity.
   Eg : Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

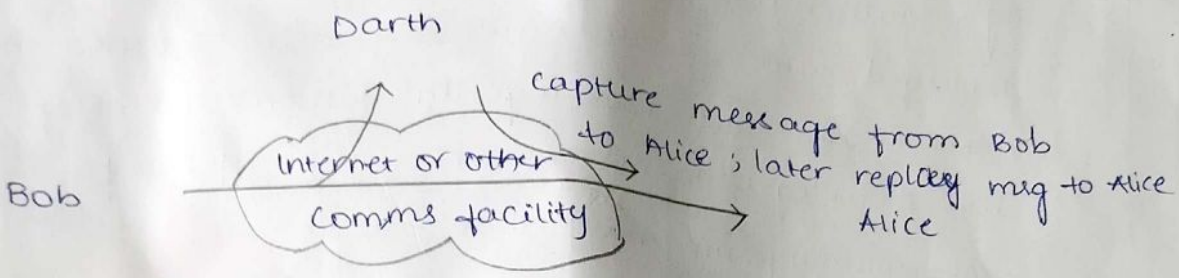
2. Replay : Involves the passive capture of a data unit and its subsequent retransmission to produce unauthorized effect.

3. Modification of message : It means that some portion of a legitimate message is altered or that messages are delayed or re-ordered, to produce an unauthorized effect.
   Eg: Message meaning "Allow John to read confidential file accounts" is modified to "Allow Fred to read confidential file accounts".

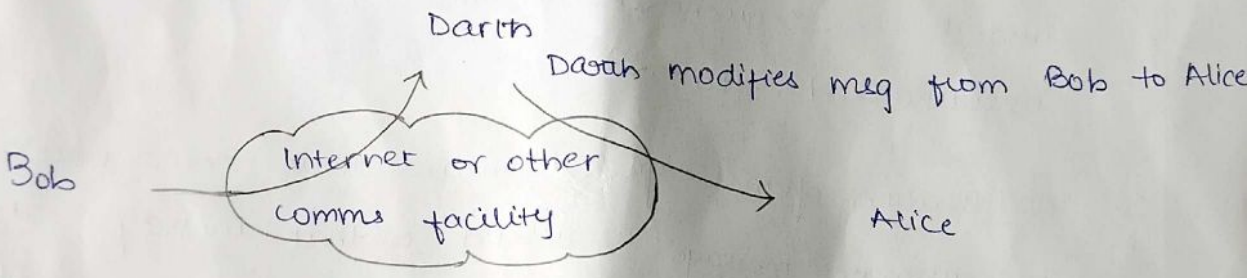
4. Denial of service : Prevents normal use or management of communications facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network, either by disabling n/w to degrade performance.



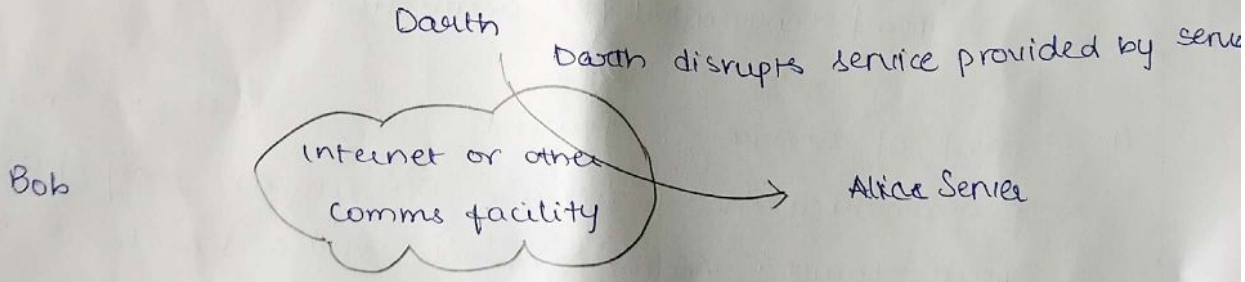
(a) Masquerade



(b) Replay



(c) Modification of messages



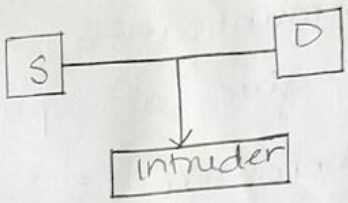
(d) Denial of service.

General Attacks

The normal flow of data from source to destination is S → D.

There are 4 general categories of attacks:

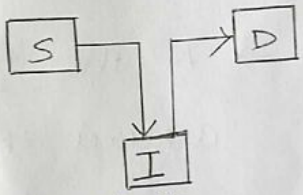
1. Interception: It is a passive attacks in which the attacker monitors and captures the message but does not change the data.



Eg: Wire tapping to capture data in N/w.

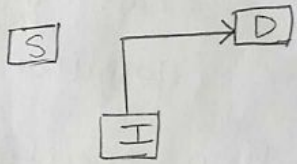
2. Interruption: It is an active attack and acts like denial of service ie., to destroy the system assets or N/w connection. Eg: Damage to some portion of hardware, cutting of a communication line or disabling of file management systems.

3. Modification: The attackers capture the message, modify and transfer it to destination.



Eg: changing values in data file, altering, modifying the contents of messages being transmitted in a network.

4. Fabrication: The attackers capture the authentication of authorized person, then getting authentication later the attackers act as authorized person sends message to destination.



Eg: Inserting additional records into a file.

SECURITY SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the system or of data transfers.

RFC 2828 defines security services as a communication service that is provided by a system to give a specific kind of protection to s/m resources.

There are 5 Security Services :

1. Authentication : The assurance that communication entity is the one that claims to be (or) the communication between two authorized person is called authentication.

   In case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved.

   → At the time of connection initiation, the service assures that the two entities are authentic ie., that each is the entity that it claims to be.

   → The service must assure that connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purpose of unauthorized transmission

Two specific authentication services are defined in X.800 :

a) Peer entity authentication : Used in association with a logical connection to provide confidence in the identity of the entities connected.

(b) Data origin authentication : In a connectionless transfer, provides assurance that the source of received data is as claimed. Eg : e-mail.

2. Access Control : Ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity is trying to gain access must first be identified (or) authenticated, so that access rights can be tailored to the individual.

3. Data Confidentiality : Protection of transmitted data from passive attacks (or) unauthorized disclosure.

→ Connection confidentiality : It is protection of all user data on a connection.

→ Connectionless confidentiality : It is protection of all user data in a single data block.

→ Selective field confidentiality : It is confidentiality of selected fields within the user data on a connection or in a single data block.

→ Traffic flow confidentiality : It is protection of information that might be derived from observation of traffic flows.

4. Data Integrity : The assurance that data recieved are exactly as sent by an authorized entity.

→ Connection Integrity with recovery : It provides for integration of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence.

with recovery attempted.

→ Connection Integrity without recovery : Provides for the Integrity of all user data on a connection and only detection without recovery.

→ Selective field connection Integrity : Provides for integrity of selected field within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.

→ Connectionless Integrity : Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.

→ Selective-field connectionless Integrity : Provides integrity of selected field within a single connectionless data block and takes form of determination of whether selected fields have been modified or not.

5. Non-Repudiation : Provides protection against denial by one of the entities involved in communication of having participated in all or part of the communication

→ Non-repudiation origin : Proves that the messages were sent by specified party.

→ Non-repudiation destination : Proves that the message were recieved by the specified party.

6. Availability Service : The data must be available to the authorized parties when they require to access them it called availability. If any 3rd party harmed, then it is not possible to access data. A service must be provided to recover from loss of availability, better solution is prevention of modification

SECURITY MECHANISMS

X.800 defines a security mechanisms as the mechanisms designed to detect, prevent or recover from a security attack. These are divided into those that are implemented in a specific protocol layer such as TCP or an application-layer protocol and those that are not specific to any particular protocol layer or security service. There are 2 types of security mechanisms:

1. Specific Security Mechanism — It may be incorporated into the appropriate protocol layer in order to provide some of the OSI security service.

   a) Encipherment :- It is the use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

   b) Digital Signature:- It is the data appended to (OL) a cryptographic transformation of a data unit that allows a reciepient of data unit to prove the source and integrity of the data unit and protect against forgery.

   c) Access Control :- A variety of mechanisms that enforce access rights to resources.

   d) Data Integrity :- A variety of mechanisms used to assure the integrity of data unit.

   e) Authentication :- A mechanism intended to ensure

the identity of an entity by means of info. exchange.

f) Traffic padding :- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

g) Routing control :- Enables selection of particular secure routes for certain data and allows routing changes especially when a breach of security is suspected.

h) Notarization :- The use of trusted 3rd party to ensure certain properties of data exchange.

2. Pervasive Security Mechanisms — The mechanisms that are not specific to any particular OSI security service (or) protocol layer.

a) Trusted Functionality :- Which is perceived to be correct w.r.t some criteria.

b) Security label :- The marking bound to a resource that names or designates the security attributes of that resources.

c) Event detection :- Detection of security relevant events.

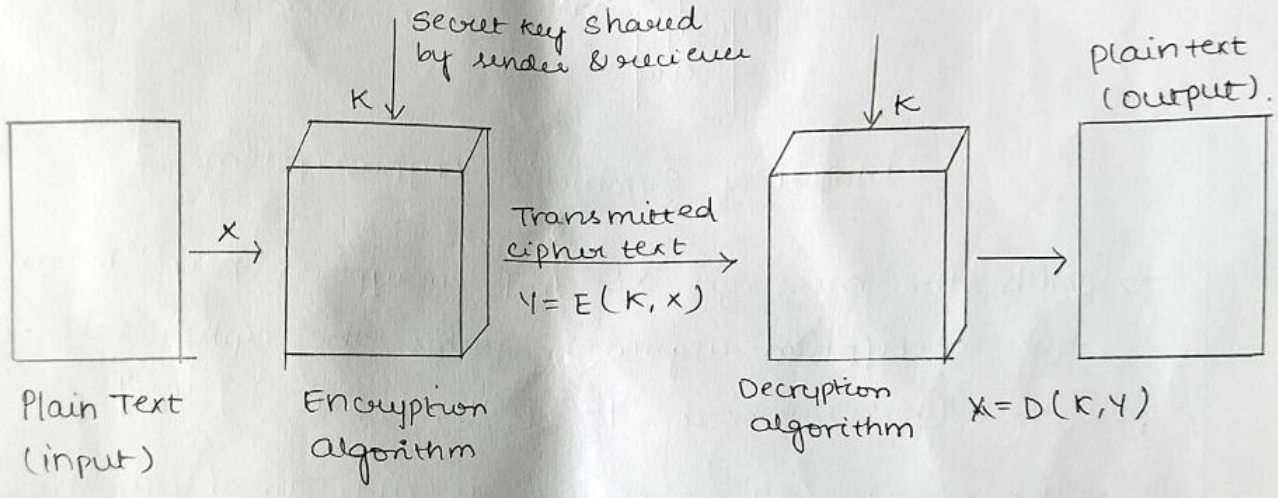
d) Security Audit Trial :- Data collected and potentially used to facilitate a security audit which is an independent review and examination of system records and activities.

e) Security Recovery :- Deals with requests from mechanisms such as event handling and management functions and takes recovery actions.

SYMMETRIC CIPHER MODEL

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using same key. It is also known as conventional encryption. A symmetric encryption scheme has 5 ingredients :

1. Plain Text — The original intelligible message or data ie., fed into algorithm as input.
2. Encryption algorithm — Performs various substitutions and transformations on plain text.
3. Secret Key — It is an encryption / decryption key known only to parties that exchange secret messages.
4. Cipher text — Apparently random stream of data and that is unintelligible. Two different keys produce two different cipher texts.
5. Decryption algorithm — Process of converting cipher text into plain text.



Simplied Model of Symmetric Encryption

There are 2 requirements for secure use of conventional encryption : 1) We need a strong encryption algorithm
2) Sender & reciever must have obtained copies of secret key in a secure fashion & must keep the key secure.

MODEL OF SYMMETRIC CRYPTOSYSTEM

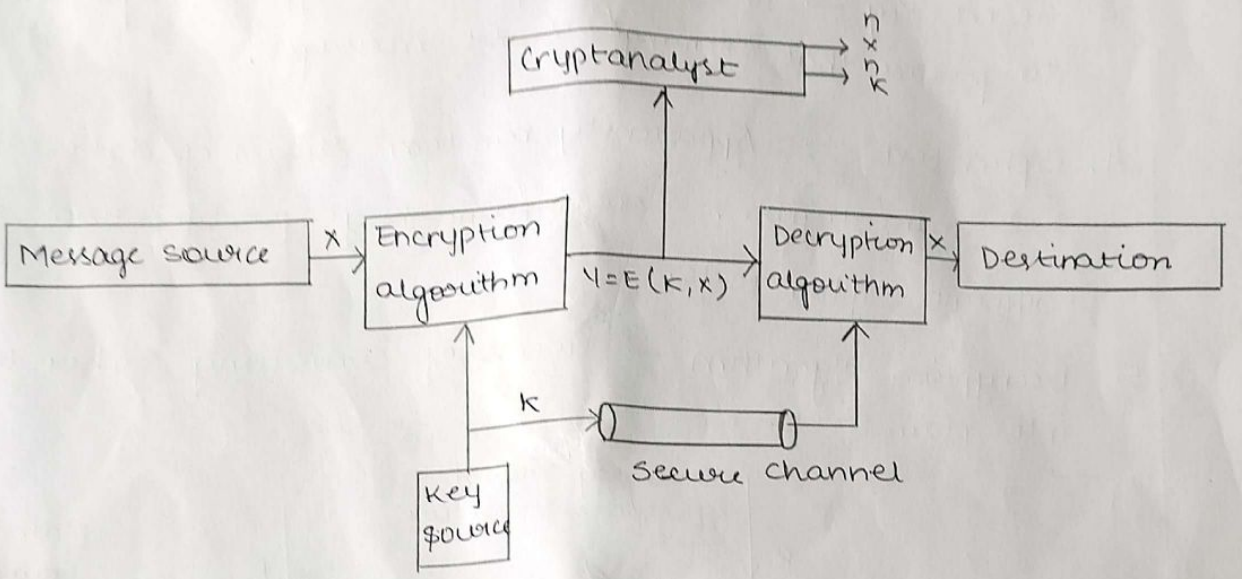
A source produces a message in plain text.

$X = \{ x_1, x_2, x_3 \ldots x_m \}$, then 'm' elements of 'X' are letters in some finite alphabet. Eg: Binary alphabet {0,1}.

For encryption, a key of the form $K = [K_1, K_2 \ldots K_j]$.

→ If the key is generated at the message source, then it must also be provided to the destination.

→ If the 3rd party generate the key, then it must be securely delivered to both source & destination.



Model of Symmetric Cryptosystem

→ With the message 'X' and encryption key 'K' as input, the encryption algorithm forms the cipher text.

$Y = E(K, X)$ where $Y = [Y_1, Y_2, Y_3 \ldots Y_n]$

→ The indended reciever is able to invert the transformations. $X = D(K, Y)$.

Cryptography : These systems are characterized along three independent dimensions.

1. Type of operations used for encryption. (Subs & trans)
2. NO. of keys used. (symmetric & asymmetric)
3. The way in which the plain text is processed. (Block & stream

CLASSICAL ENCRYPTION TECHNIQUES

The two basic building blocks of all encryption techniques are substitution and transposition. In substitution, letters are replaced by other letters. In transposition, the letters are arranged in diff. order. These are classified as:

1) Monoalphabetic – only 1 character is replaced by single character.
2) Polyalphabetic – several substitutions are used.

SUBSTITUTION TECHNIQUES :

Here, letters of plaintext are replaced by other letters or by numbers or symbols. If plain text is viewed as a sequence of bits then substitution involves replacing plain text bit patterns with cipher bit patterns.

1. Caeser Cipher – Involves replacing each letter of the alphabet with the letter standing in their places. It is also called as shifted alphabet cipher. Let us assign numerical equivalent to each letter.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows:
For each plain text letter P, substitute the cipher text letter C:

$C = E(3, P) = (P+3) \bmod 26$ where $K = 3$;

A shift may be any amount, so that the general caesar algorithm is

$C = E(K, P) = (P+K) \bmod 26$.

where K takes on a value in the range 1 to 25.

The decryption algorithm is

$P = D(K, C) = (C-K) \bmod 26$

Eg: Plaintext is GVPCEW.

$C = E(3, G) = (6+3) \bmod 26 = 9 = J$

$C = E(3, V) = (3+21) \bmod 26 = 24 = Y$

Cipher text: JYSFHZ

$P = D(J-3) = (9-3) \bmod 26 = 9$

$P = D(Y-3) = (24-3) \bmod 26 = V$

2. Playfair Cipher :- It is based on the use of a 5×5 matrix of letters constructed using a keyword. Here, the matrix is constructed by filling in letters of the keyword from left to right and top to bottom and then filling in the remainder of the matrix with the remaining letters in alphabetic order. (Excluding repeated letters). Here 'I', 'J' are considered as one unit. Eg: MONARCHY

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

Eg: GVPCEW.

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

Plain text is encrypted two letters at a time, according to the following rules :

1. Repeating plaintext letters that are in same pair are seperated with filler letter such as 'x' so that balloon would be treated as bal x lo on.
2. Two plaintext letters that fall in the same row of the matrix are replaced by letter to right with the first element of the row circularly following the last.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. Eg: MU is encrypted as EM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and column occupied by the other plaintext letter. Eg: hs becomes BP; ea becomes IM or JM is example MONARCHY.

Eg: Message – SECRET MESSAGE
Key – Keyword.

Rules : 1) Must split your message into pairs
2) Seperate all duplicated letters by inserting 'x'.
3) Ignore all spaces.

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

SE CR ET ME SX SA GE

SE → It forms rectangle. NO
CR → It forms same row, then takes move each letter right. RD
ET → forms rectangle KU
ME → forms rectangle NK
SX → forms rectangle QZ
SA → forms rectangle PC
GE → forms same column so it moves down. ND

Ciphertext : NORD KUNK QZ PC ND

Decryption is as follows above and take cipher text and keyword as input.

3. Hill Cipher: (1921)

It is based on linear algebra / equation. This technique uses either 2x2 (or) 3x3 matrix. Here, we select a key that must follow $K \cdot K^{-1} = K^{-1} \cdot K = I$. Where $K^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod 26$

$C = \Sigma(K, P) \bmod 26 = KP \bmod 26$

$P = D(K, C) = CK^{-1} \bmod 26.$

Eg: Given character set:

A	B	C	D	E	F	G
0	1	2	3	4	5	6
a	b	c	d	e	f	
7	8	9	10	11	12	
0	1	2	3			
13	14	15	16			
*	&	!	}			
17	18	19				

Message: Aa!oFa

Key: $\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$

Find out cipher text.

Sol: The message will be divided into three equal blocks.

Aa | !o | Fa. (Plain Text as column vectors)

$c(Aa) = \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 7 \end{bmatrix} \bmod 20 = \begin{bmatrix} 7 \\ 28 \end{bmatrix} \bmod 20 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = (ab)$

$c(!o) = \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 19 \\ 13 \end{bmatrix} \bmod 20 = \begin{bmatrix} 12 \\ 9 \end{bmatrix} = (fc)$

$c(Fa) = \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 \\ 7 \end{bmatrix} \bmod 20 = \begin{bmatrix} 12 \\ 3 \end{bmatrix} = (fD).$

∴ Cipher text : ab fc fD

Decryption :- $K^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod 20.$

$K^{-1} = \frac{1}{4-3} \begin{bmatrix} 4 & -1 \\ -3 & 1 \end{bmatrix} \bmod 20 = \begin{bmatrix} 4 & -1 \\ -3 & 1 \end{bmatrix} \bmod 20$

$= \begin{bmatrix} 4 & 19 \\ 17 & 1 \end{bmatrix}$

$$P(ab) = \begin{bmatrix} 4 & 19 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 20 = \begin{bmatrix} 0 \\ 7 \end{bmatrix} = (Ha)$$

$$P(fc) = \begin{bmatrix} 4 & 19 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 9 \end{bmatrix} \bmod 20 = \begin{bmatrix} 19 \\ 13 \end{bmatrix} = (!o)$$

$$P(fD) = \begin{bmatrix} 4 & 19 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 3 \end{bmatrix} \bmod 20 = \begin{bmatrix} 5 \\ 7 \end{bmatrix} = (Fa)$$

Plain Text : Aa !o Fa

4. Polyalphaberic Ciphers — involves series of monoalphaberic ciphers that are periodically reused. There are diff. methods:

→ Vigenere Ciphers :

Blaise de Vigenere, a french cryptographer of the 15th century created this cipher. It has similar method of encryption as Caeser Cipher but uses a more complex encryption key. It is a more secure cipher than Caeser Cipher. The plaintext is enciphered using a string instead of a singular number or letter. Each alphabetic character in plaintext is shifted by the letter in the keyword.

$C = E(P,K) \bmod 26 = (P+K) \bmod 26$

$P = D(C,K) \bmod 26 = (C-K) \bmod 26.$

Eg: Message — MEET ME TOMORROW.

Key — TRIALS

Plain Text :	M	E	E	T	M	E	T	O	M	O	R	R	O	W	
Numerical :	12	4	4	19	12	4	19	14	12	14	17	17	14	22	
Key :	T	R	I	A	L	S	T	R	I	A	L	S	T	R	
Numerical :	19	17	8	0	11	18	19	17	8	0	11	18	19	17	
Cipher Num :	5	21	12	19	23	22	12	5	20	14	2	9	7	13	
Cipher Text :	F	V	M	T	X	W	M	F	U	O	C	J	H	N	

Decryption:

Cipher text:	F	V	M	J	X	W	M	F	U	O	C	J	H	N	
Numerical:	5	21	12	19	23	22	12	5	20	14	2	9	7	13	
Key:	T	R	I	A	L	S	T	R	I	A	L	S	T	R	
Numerical:	19	17	8	0	11	18	19	17	8	0	11	18	19	17	
Plain Text Num:	12	4	4	19	12	4	19	14	12	14	17	17	14	22	
Plain Text:	M	E	E	T	M	E	T	O	M	O	R	R	O	W	

→ Vernam Cipher — Was introduced by AT&T engineer named Gilbert Vernam in 1918. It works on binary data rather than letters. It is expressed as

Encryption $C_i = P_i \oplus K_i$

where C_i – ith binary digit of ciphertext

P_i – ith binary digit of plaintext.

K_i – ith binary digit of key.

$\oplus$ – exclusive or (XOR) operation.

Decryption $P_i = C_i \oplus K_i$

5. One time pad (OTP) — Also known as vernam cipher or perfect cipher is a crypto algorithm where plaintext is combined with a random key. It is the only existing mathematically unbreakable encryptions.

Rules: 1) Key is same size as that size of plain text.

2) Key is truly random (No pseudo random functions.

3) Key should be used only once (destroy after use).

4) There are only two copies of keys (1 for sender and other for reciever).

• encryption:

plain text : HELLO
key : XMCKL
EQNVZ

7	4	11	11	14
23	12	2	10	11
4	16	13	21	25

plain text : HELLO
key : RSUDC
YWFOQ

7	4	11	11	14
17	18	20	3	2
24	22	5	14	16

For decryption, subtract the key from cipher text.

TRANSPOSITION CIPHER TECHNIQUES

Here, it simply moves letters around rather than replacing them with something else.

Transposition encryption :

plain text — MEET ME TOMORROW
Cipher text — TEEM EM WORROMOT

→ Rail fence cipher : Here plain text is written down as sequence of diagonals & then read as a sequence of row ie., it involves writing a message in diagonal format in a grid.

Encryption — Plain text : TEXTBOOK PAGE THREE

T	-	-	-	B	-	-	-	P	-	-	-	T	-	-	-	E
-	E	-	T	-	O	-	K	-	A	-	E	-	H	-	E	-
-	-	X	-	-	-	O	-	-	-	G	-	-	-	R	-	-

Cipher text produced : TBPTEETOKAEHEXOGR

Decryption is done by arranging them in the grid horizontally.

→ Route Cipher —

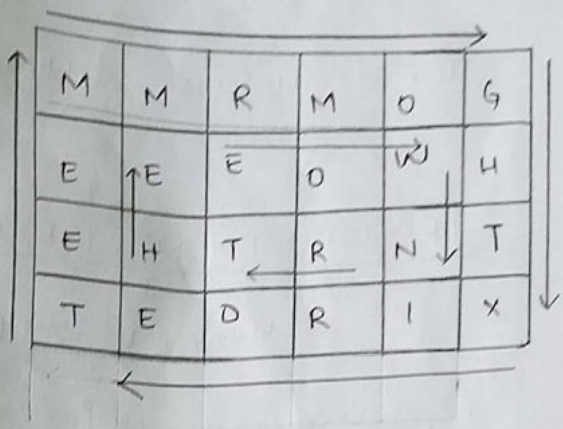
Here, message is written in the form of a rectangle, choosing a route around the grid.

Encryption: plain text is

MEET ME HERE TOMORROW NIGHT

1) Key should start point should be to the bottom left and in clockwise direction.

2) If empty box is there, fill it with 'x'.



M	M	R	M	O	G
E	E	E	O	W	H
E	H	T	R	N	T
T	E	D	R	I	X

Cipher text is:

TEEMMRMOGHTJXIROEHEEOWNRT

Decryption: ~~Same as above but in anti-clockwise direction.~~

We can decrypt the message by adding cipher text to the table.

CYBER THREATS AND THEIR DEFENSE

Cyber threat is the possibility of a malicious attempt to damage a computer network.

Types :

1) Device Compromise — To obtain total control of a device.
2) Service Disruption — To prevent a device from performing its duties.
3) Data Ex-filteration — To steal sensitive information from target.
4) Bad Data Injection — To submit incorrect data to a system without detection.
5) Advanced persistant threats — To gain extended access of a device.

General Cyber threats :

1) Distributed Denial of service (DDOS) — A Denial of service (DOS) attack where multiple compromised systems which are often infected with a Trojan, are used to target a single system.

Note : What is the difference between DoS and DDoS attacks?

A DoS attack typically uses one computer and one internet connection to flood a targeted system whereas a DDoS attack uses multiple computers and internet connections to flood the targeted systems.

Types of DDoS attacks are:

1) Traffic attacks
2) Bandwidth attacks
3) Application attacks

2) Brute Force attack — This attack consists of an attacker trying many passwords with the hope of eventually guessing correctly. The attacker checks all the possible passwords until correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using key-derivation function. This is known as exhaustive key search.

When a single password is tested against multiple usernames or encrypted files, it is called reverse brute-force attack.

Attack Artifacts :

They are used to destroy systems.

1) Virus
2) Worms
3) Trojan Horse
4) Denial of Service.

Defenses :

1) Patching - To update system software
2) Anti-Virus - designed to detect and destroy computer viruses. Eg : K7, Kaspersky.
3) Firewall - To protect from unauthorized access

4) Intruder - Detection System - Type of security software designed to automatically alert administrators when someone or something is trying to compromise information information system through malicious activities.

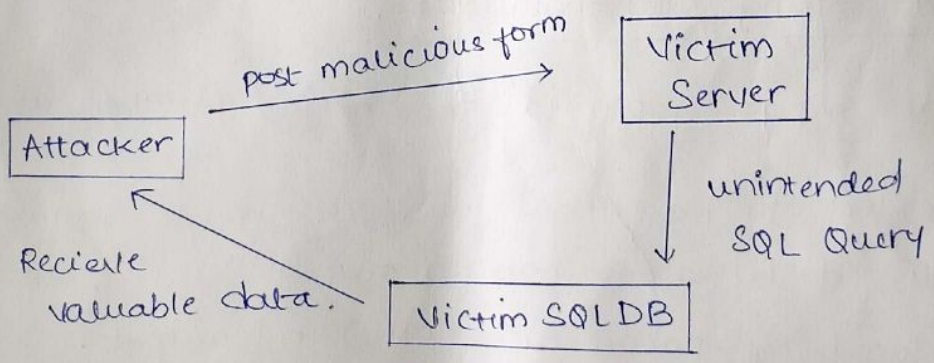
5) Gateway - Checks whether authorized person accesses or not based on input.

* Phishing Defensive Measures

Phishing is the attempt to obtain sensitive information such as username, password and credit card details, often for malicious reasons by masquerading as a trustworthy entity in an electronic communication. It is a continual threat and the risk is even larger in social media such as FaceBook, Twitter and Google+. Hackers could create a clone of website and tell you to later enter personal information, which is then emailed to them.

* SQL injection and Defense Techniques

- Browser sends malicious input to server.
- Bad input checking leads to malicious SQL Query.



We can prevent SQL injection by:

Never using building SQL commands ourself.

- Use parameterized / prepared SQL.
- Use ORM framework.

* Buffer Overflow

Also called as buffer overrun is an anomaly where a program, while writing data to a buffer overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of violation of memory safety.

Buffer Overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. This may result in erratic program behaviour including memory access errors, incorrect results, a crash or a breach of system security. Eg: Stack Buffer overflow.

A buffer overflow occurs when data written to a buffer also corrupts data values in memory addresses adjacent to destination buffer due to insufficient bounds checking. This can occur when copying data from one buffer to another without first checking that the data fits within the destination buffer.

Format String Vulnerabilities.

Format String : printf ("The magic number is :%d \n", 1911);

The text to be printed is "The magic number is :", followed by a format parameter '%d', which is replaced by parameter (1911) in output.

Format String Vulnerabilities are the result of programmers allowing externally supplied, unsanitized data in the format string argument. The best solution to format string vulnerabilities is prevention.

* TCP Session Hijacking

When attempting to hijack a TCP connection, a hacker must pay attention to all the details that go into a TCP connection. These details include things like sequence numbers, TCP headers and ACK packets.

If an attacker is able to perform a TCP session hijack in such a way that he completely controls the transmission of packets between the two hosts, that attacker has a considerable advantage.

Route Table Modification :

An attacker would be able to put himself in such a position to block packets by modifying routing tables so that packets flow through a system he has control of, by changing bridge tables by playing games with spanning tree frames.

Most of the time, an attacker will try to change route tables remotely. There has been some research in the area of changing route tables on a mass scale by playing games with the Border Gateway Protocol (BGP) that most Internet Service Providers use to exchange routes with each other.

ARP Attacks :

Another way to make sure that your attacking machine gets all the packets going through it is to modify the ARP tables on victim machine.

An ARP table controls the Media Access Control (MAC)-address - to - IP - address mapping on each machine. ARP is designed to be a dynamic protocol. There is absolutely no authentication in this protocol.

When a victim machine broadcasts for MAC address that belongs to a particular IP address, all an attacker has to do is answer before the real machine being requested does. It is a classical race condition.

A tool for performing an ARP attack is (for a lack of formal name) grat-arp, by Mudge (and he claims, some unidentified friends).

ARP tricks are good not only for getting traffic to flow through your machine, but also just so you can monitor it at all when you're in a switched environment. Normally, when there is a switch between the victim and attacking machine, the attacking machine will not get to monitor the victim's traffic

* UDP Hijacking

A UDP Hijacker creates a state wherever the shopper and server square measure unable to exchange information, so he tries to forge acceptable packets for each ends, that acts because of real packets. UDP Hijacking is better than TCP because it does not have the complexity of managing TCP Security