Network and Information Security
Lecture 1

B.Tech. Computer Engineering
Sem. VI.

M. T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Books:

- Cryptography and Network Security, William Stallings
- Cryptography and Network Security, Behrouz Forouzan and Debdeep Mukhopadhyay

Introduction

- Information is an asset that has a value like any other asset.
- As an asset, information needs to be secured from attacks.
- Security Goals
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

- We need to protect out confidential information.
- Military-Concealment of sensitive information is a major concern.
- In, Industry, hiding information from competitors is crucial to the operation of the organization.
- In banking, customer's account needs to be kept secret.
- When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.
- Cryptography can achieve confidentiality aspect of security.

Integrity

- Information needs to be changed constantly.
- In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information.
- Integrity aspect is taken care by Hashing algorithms. e.g SHA-256, MD-5

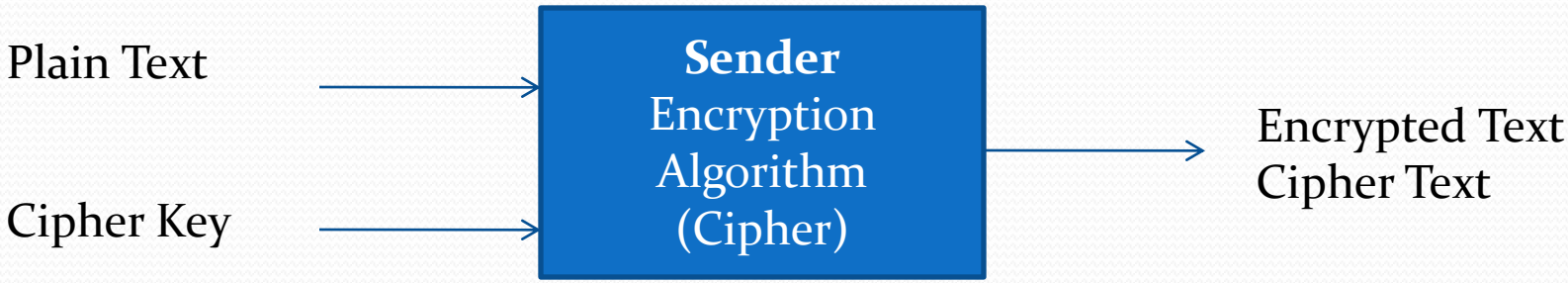
Availability

- The information created and stored by an organization needs to be available to authorized entities.
- Information is useless if it is not available.
- Information needs to be constantly changed, which means it must be accessible to authorized entities.
- The unavailability of information is harmful.
  - What would happen to a bank if customer could not access their accounts for transaction.
- E.g. Denial of service attack (DOS attack) – It may slow down or totally interrupt the service of a system.

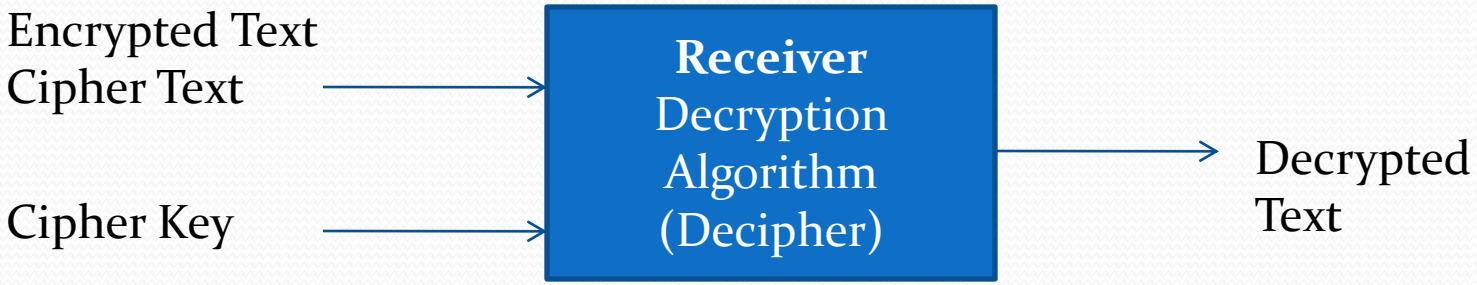
- Confidentiality
- If a sender sends a text message to the receiver then receiver should receive concealed text message.
- If unauthorized person receives then the message is hidden.
- Encryption is the way to convert original message to a form which can't be easily decoded by unauthorized person.

Terminology

- Original message- Plain Text
- Cipher Key –Key
- Cipher – Encryption Algorithm
- Cipher Text – Output of encryption algorithm



- Generally Key is shared secret between sender and receiver only.



- Decrypted text is same as plain text or must be same as plain text.

- If the secret key is guessed or discovered by someone, then cipher text is decrypted and confidentiality is violated.

Example: Additive Cipher/ Shift Cipher

- The simplest monoalphabetic cipher is the additive cipher.
- Also called as, Shift cipher or Caesar cipher
- Symmetric cipher category
- Algorithm
- C= (P + k) MOD 26
- C=Number corresponding to the cipher text character
- P=Number corresponding to the plain text character
- Assume, Alphabet set
- ∑ = { a,b,c,d,……,x,y,z}

Mapping

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
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

Suppose Plain Text =“Welcome”, Key=5 (Randomly selected from 0 to 25)
Key must be shared between sender and receiver.

W	E	L	C	O	M	E
22	4	11	2	14	12	4

- $C_i = (P_i + k) \bmod 26$

Plain Text	w	e	l	c	o	m	e
Plain text mapping	22	4	11	2	14	12	4
Key	5	5	5	5	5	5	5
Plain Text +Key	27	9	16	7	19	17	9
(Plain Text +Key) % 26	1	9	16	7	19	17	9
Cipher Text	B	J	Q	H	T	R	J

- Receiver Side decryption
- $P_i = (C_i - k) \bmod 26$

Cipher Text	B	J	Q	H	T	R	J
Cipher text mapping	1	9	16	7	19	17	9
Key	5	5	5	5	5	5	5
Cipher Text – Key	-4	4	11	2	14	12	4
(Cipher Text -Key) Mod 26	22	4	11	2	14	12	4
Plain Text	w	e	l	c	o	m	e

- To perform
- (-4) mod 26
- (-4) divided by 26
- 26 multiply (-1) = (-26)
- (-4) - (-26) = 22

- Cryptanalysis
- Additive cipher are vulnerable to cipher-text only attacks using exhaustive key searches (brute-force attacks)
- The key domain of the additive cipher is very small. Only 26 keys.
- K=0 is not possible (P=C)
- There are only 25 possible keys.