Network and Information Security
Lecture 2

B.Tech. Computer Engineering
Sem. VI.

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

Cryptographic Attacks

- Cryptanalytic attacks
- Combinations of statistical and algebraic techniques aimed at ascertaining the secret key or a cipher.
- Cryptanalysis: the attacker guesses the key and looks for the distinguishing property.
- If the property is detected, the guess is correct otherwise the next guess is tried.
- Brute force search method for guessing key
- Divide-and-Conquer method for guessing key (Efficient)
- Also, used to find a flaw in the design

- Non-Cryptanalytic attacks
- Do not exploit the mathematical weakness of the cryptographic algorithm.
- 3 goals of security are threatened by this class
- Attacks threatening confidentiality
- Snooping –unauthorized access to or interception of data
  - prevented by encipherment technique
- Traffic analysis- although encipherment of data may make it nonintelligible for the interceptor, she can obtain some other type of information by monitoring online traffic.
  - E.g. Find the email address of sender and receiver and guess the nature of transaction

- Attacks threatening Integrity
- Modification – after intercepting information, the attacker modifies the information to make it beneficial to herself
- Masquerading (spoofing) – the attacker impersonates somebody else. E.g. Stealing of bank ATM card and PIN of a customer
- Replaying – the attacker obtains the copy of a message sent by a user and later tries to replay it
- Repudiation-the sender of the message might later deny that she has sent the message, the receiver of the message might later deny that he has received the message

- Attacks threatening availability
- Denial of service
- It may slow down or totally interrupt the service of a system.
- The attacker might send so many bogus requests to a server that the server crashes because of the heavy load
- The attacker might intercept and delete a server's responses to a client, making the client to believe that the server is not responding or attacker may intercept requests of a client, causing the clients to send requests many times and overload the system

- Passive versus Active Attacks
- Passive attacks-
- the attack does not modify the data or harm the system
- however, the attack may harm sender or the receiver of the message
- E.g. Snooping and traffic analysis
- It is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential information
- It can be prevented by encipherment of the data

- Active attack may change the data or harm the system
- E.g. Modification, masquerading, replaying, repudiation
- Easier to detect than to prevent

- Example 1:
- Use the Additive cipher with Key=15 to encrypt the message “hello”.

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 =“hello”, Key=15
Key must be shared between sender and receiver.

h	e	l	l	o
7	4	11	11	14

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

Plain Text	h	e	l	l	o
Plain text mapping					
Key					
Plain Text +Key					
(Plain Text +Key) % 26					
Cipher Text					

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

Plain Text	h	e	l	l	o
Plain text mapping	7	4	11	11	14
Key	15	15	15	15	15
Plain Text +Key	22	19	26	26	29
(Plain Text +Key) % 26	22	19	0	0	3
Cipher Text	W	T	A	A	D

- Example 2
- Use the additive cipher with key=15 to decrypt the message “WTAAD”

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

Cipher Text	W	T	A	A	D
Cipher text mapping					
Key					
Cipher Text – Key					
(Cipher Text -Key) Mod 26					
Plain Text					

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

Cipher Text	W	T	A	A	D
Cipher text mapping	22	19	0	0	3
Key	15	15	15	15	15
Cipher Text – Key	7	4	-15	-15	-12
(Cipher Text -Key) Mod 26	7	4	11	11	14
Plain Text	h	e	l	l	o

- Example 3
- Eve has intercepted the ciphertext “UVACLYFZLJBYL”.
- Show how she can use a brute-force attack to break the cipher.
- Take k=1,2,3,4,5,6,7,….,25 and Convert Cipher Text to Plain text.
- k=1 (tuzbkxeykiaxk), k=2(styajwdxjhzwj), k=3(rsxzivcwigyvi), k=4(qrwyhubvhfxuh),
- K=5(pqvxgtaugewtg),k=6(opuwfsztfdvsf)

- Take k=1,2,3,4,5,6,7,….,25

Cipher Text	U	V	A	C	L	Y	F	Z	L	J	B	Y	L
Cipher text mapping													
Key													
Cipher Text – Key													
(Cipher Text -Key) Mod 26													
Plain Text													

Cipher Text	U	V	A	C	L	Y	F	Z	L	J	B	Y	L
Cipher text mapping	20	21	0	2	11	24	5	25	11	9	1	24	11
Key	7	7	7	7	7	7	7	7	7	7	7	7	7
Cipher Text – Key	13	14	-7	-5	4	17	-2	18	4	2	-6	17	4
(Cipher Text -Key) Mod 26	13	14	19	21	4	17	24	18	4	2	20	17	4
Plain Text	n	o	t	v	e	r	y	s	e	c	u	r	e