Date __/__/__

Tutorial Sheet - 01

KAHKASHA KHAN, 19BCS013

Q-1 There are three major goals of network security :-

(i) confidentiality : we need to protect our confidential info. An organization needs to guard against those malicious activities that endanger the confidentiality of its information.

(ii) Integrity : Integrity means that changes need to be done only by authorized entities & through authorized mechanisms.

(iii) Availability : The information created & stored by an organisation needs to be available to authorized entities. The unavailability of information is just as harmful for an organisation as the lack of confidentiality or integrity.

- Taxonomy of attacks with relation to security goals :-

Threat to confidentiality : Snooping, Traffic analysis

Threat to Integrity : Modification, Masquerading, replaying, Repudiation

Threat to availability :- Denial of service

Page No.

KAMKASHA KHAN
19BCS013

Date ___/___/___

:- Attacks threatening confidentiality

- Snooping :- It refers to unauthorized access to or interception of data.
- traffic analysis : When interceptor obtain some other type of information by monitoring online traffic.

:- Attacks threatening Integrity

- Modification :- After intercepting information, the attacker modifies the info. to make it beneficial to themselves.
- Masquerading :- Masquerading or spoofing happens when the attacker impersonates somebody else
- Replaying :- Here the attacker obtains a copy of a message sent by a user & later tried to replay it.
- Repudiation :- This type of attack is performed by one of the two parties in the communication : the sender or the reciever. 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.

Page No.

Date ___/___/___

KAHKASHA KHAN
19BCS013

Q:- Attacks threatening Availability

- Denial of Service : DoS is a very common attack. It may slow down or totally interrupt the service of a system.

Q-2 Security Mechanisms :-

Encipherment
Data Integrity
Digital Signature
Authentication Exchange

Traffic padding
Routing control
Notarization
Access control

- Encipherment : Encipherment, hiding or covering data can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Two techniques cryptography & stagnography are used for encipherring.

- Data Integrity : The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.

- Digital Signature : A digital signature is a means by which the sender can electronically sign the data & the reciever can electronically verify the signature.

Page No.

Date __/__/__

KAHKASHA KHAN
19BCS013

- Authentication Exchange : Here, two entities exchange some messages to prove their identities to each other.

- Traffic Padding : It means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

- Routing Control : Means selecting & continuously changing different available routes between the sender & the reciever to prevent the opponent from eavesdropping on a particular route.

- Notarization : It means selecting a third trusted party to control the communication between two entities. This can be done, eg. to prevent repudiation.

- Access Control : It uses methods to prove that a user has access right to the data or resources owned by a system.

Q-3. The word steganography with origin in greek means covered writing in contrast with cryptography which means secret writing. Steganography means concealing the ~~contents~~ of unencrypted itself by covering it with something else.

Date __/__/____

KAHKASHA KHAN
15BCS013

We'll use a dictionary of words organized acc. to their grammatical usage. We can have a dictionary containing 2 articles, 8 verbs, 32 nouns & 4 prepositions. Suppose that we agree to use cover text that always use sentence with the pattern article-noun-article-noun. The secret binary data can be divided into 16 bit chunks

A friend called a doctor
0 10010 0001 0 01001.

Hi is 0100100001001 001

A-4 Categorization of passive & active attacks

Attacks	Type	Threatening
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity.
Denial of service	Active	Availability.

Page No.

KAHKASHA KHAN
19BCS013

- Passive Attacks : In a passive attack, the attacker's goal is just too obtain information. This means that the attack does not modify data or harm the system. The system continues with its normal operation. However, the attack may harm the sender or reciever of the message. Attacks that threaten confidentiality – snooping & traffic analysis are passive attacks. Passive attacks can be prevented by encipherment of data.

- Active Attacks : An active attack may change the data or harm the system. Attacks that threaten the integrity & availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in variety of ways.

Q-5 i) Packet sniffing :- A packet sniffing attack or simply a sniffing attack is a cyber attack that involves intercepting & misusing content (like reading sensitive data) passing through a network in the form of packets. Unencrypted email communications, login passwords & financial information are common targets for a packet sniffing attack. Besides this, an attacker may also use sniffing tools to hijack packets by injecting malicious code into the packet itself, which executes once it reaches the target device.

Date ___/___/___

KAHKASHA KHAN 7th Class
19BCS013

(ii) Packet spoofing : Also known as IP spoofing is the creation of internet protocol (IP) packet having a source IP address with the purpose of concealing the identity of the sender or impersonating another computing system. A spoofing attack occurs when a malicious party impersonates another device or user on a network in order to launch attack against network hosts, steal data, spread malware, or bypass access controls

(iii) DNS Spoofing :- Domain Name Service spoofing is the process of poisoning entries on a DNS server to redirect a targeted user to a malicious website under attacker control. The DNS attacks typically happens in a public wifi environment but can occur in any situation where the attacker can poison ARP (Address Resolution Protocol) tables & force targeted user devices into using the attacker controlled machine as the server for a specific website. It's the first step in a sophisticated phishing attack on public wifi & it can also trick users into installing malware on their devices or divulge sensitive information.

KAHKASHA KHAN
19BCS013

Date ___/___/___

Ques-6 We can divide traditional symmetric key ciphers into two broad categories :

1) Substitution cipher 2) transposition cipher

1) Substitution cipher :- Here we replace one symbol in the ciphertext with another symbol

a) Monoalphabetic cipher :- Here a character in the plaintext is always changed to same character in the ciphertext regardless of its position in the text.

b) • Additive cipher :- Simplest monoalphabetic ciphers. also known as Shift or caeser ciphers.

Encryption : $C = (P + K) \bmod 26$.

Decryption : $P = (C - K) \bmod 26$

• Multiplicative cipher :-

Encryption : $C = (P * K) \bmod 26$

Decryption : $P = (C * K^{-1}) \bmod 26$

K^{-1} :- multiplicative inverse.

• Affine Cipher : we combine the additive & multiplicative ~~inverse~~ ciphers to get what is called the affine cipher - a combination of both ciphers with a pair of keys.

Encryption : $C = (P * K_1 + K_2) \bmod 26$

Decryption : $P = ((C - K_2) * K_1^{-1}) \bmod 26$

Date ___/___/___

KAHKASHA KHAN
19BCS013

b) Polyalphabetic ciphers:- Here each occurence of a character may have a different substitute.

- Autokey cipher: In this cipher, the key is a stream of subkeys in which each subkey is used to encrypt the corresponding character in the plaintext.

$P = P_1 P_2 P_3 \cdots \quad C = C_1 C_2 C_3 \cdots \quad K = (k_1, P_1, P_2 \cdots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$

Decryption: $P_i = (C_i - k_i) \bmod 26$

- Playfair Cipher: The secret key is made of 25 alphabets letters arranged in a 5×5 matrix. (letters I & J are considered same)

Before encryption, if the 2 letters pair are same we add a bogus letter to seperate them. After inserting bogus letter if no. of character is odd one extra bogus character is added to end make it even.

$P = P_1, P_2 P_3 \quad C = C_1 C_2 C_3 \quad K = [(k_1, k_2), (k_3, k_4), \cdots]$

Encryption: $C_i = k_i \quad$ Decryption $P_i = k_i$

- Vigenere cipher:- Here the key stream is a repetition of an initial secret key stream of length m, where we have $1 \le m \le 26$.

$P = P_1 P_2 P_3 \quad C = C_1 C_2 C_3 \quad K = [(k_1, k_2, \cdots, k_m), (k_1, k_2 \cdots k_m) \cdots]$

Encryption: $C_i = P_i + k_i$

Decryption: $P_i = C_i - k_i$

Page No.

19BCS013
KAHKASHA KHAN

Date __/__/__

- Hill cipher :- unlike other polyalphabetic ciphers, here the plaintext is divided into equal sized blocks. Here, the key is a square matrix of size m×m where m is the size of the block.

If we call the m characters in the plaintext block $P_1, P_2, \ldots P_m$ the corresponding characters in the ciphertext block are $C_1, C_2, \ldots C_m$ then we have

$$C_1 = P_1K_{11} + P_2K_{21} \ldots + P_mK_{m1}$$
$$\ldots$$
$$C_m = P_1K_{1m} + P_2K_{2m} + \ldots + P_mK_{mm}$$

the equations show that each ciphertext character such as C_1 depends on all plaintext characters

- Rotor Cipher :- It uses the idea behind mono alphabetic substitution but changes the mapping between the plaintext & the ciphertext characters for each plain text character.

~~Enigma machine is~~

b) Transposition Ciphers :- Changes location of the symbols

- Keyless Transposition ciphers :- There are 2 methods for permutation of characters. i) text is written col-by col & transmitted row by row or vice versa

- Keyed Transposition cipher :- It permutes the character by writing plaintext in one way (row by row, from) & reading it another way (col by col, for eg)

Page No.

Date ___/___/___

KAMKASHA KHAN
15BCS013

Q-7 ab → GL means 00 → 06 & 01 → 11

constructing equations

$0 \times k_1 + k_2 = 6 \pmod{26}$ — (1)

$1 \times k_1 + k_2 = 11 \pmod{26}$ — (2)

solving (1) & (2) we get

$k_1 = 5$ & $k_2 = 6$.

this means

$P = ((C - k_2) \times k_1^{-1}) \bmod 26$

$= ((C + 20) \times 21) \bmod 26$

upon solving we get plain text :—

P: the best of a fight is making up afterwards

Date ___/___/___

KAHKASHA KHAN
19BCS013

Q-8. Plain text = "This is an exercise"

Additive Cipher : key = 20.

T	(19 + 20) mod 26	⇒ 13	⇒ N
H	(7 + 20) mod 26	⇒ 1	⇒ B
I	(8 + 20) mod 26	⇒ 2	⇒ C
S	(18 + 20) mod 26	⇒ 12	⇒ M
I	(8 + 20) mod 26	⇒ 2	⇒ C
S	(18 + 20) mod 26	⇒ 12	⇒ M
A	(0 + 20) mod 26	⇒ 20	⇒ U
N	(13 + 20) mod 26	⇒ 7	⇒ H
E	(4 + 20) mod 26	⇒ 24	⇒ Y
x	(23 + 20) mod 26	⇒ 17	⇒ R
E	(4 + 20) mod 26	⇒ 24	⇒ Y
R	(17 + 20) mod 26	⇒ 11	⇒ L
C	(2 + 20) mod 26	⇒ 22	⇒ W
I	(8 + 20) mod 26	⇒ 2	⇒ C
S	(18 + 20) mod 26	⇒ 12	⇒ M
E	(4 + 20) mod 26	⇒ 24	⇒ Y

cipher text : NBCM CM UHY RYL WCMY.

Date ___/___/___

KAHKASHA KHAN
18BCS2018

~~cipher text~~

Multiplicative cipher : key = 15.

T	(19 x 15) mod 26	25	Z
H	(7 x 15) mod 26	1	B
I	(8 x 15) mod 26	16	Φ
S	(18 x 15) mod 26	10	K
I	(8 x 15) mod 26	16	Φ
S	(18 x 15) mod 26	10	K
A	(0 x 15) mod 26	0	A
N	(13 x 15) mod 26	13	N
E	(4 x 15) mod 26	8	I
X	(23 x 15) mod 26	7	H
E	(4 x 15) mod 26	8	I
R	(17 x 15) mod 26	21	V
C	(2 x 15) mod 26	4	E
I	(8 x 15) mod 26	16	Φ
S	(18 x 15) mod 26	10	K
E	(4 x 15) mod 26	8	I

cipher text : ZBΦKΦKANIHIVEΦKI

Date ___/___/___

KAMKASHA EMAN
18BCS013

c) AFFINE CIPHER :- key (15, 20)

T	$(19 \times 15) + 20 \bmod 26$	19	T
H	$(7 \times 15) + 20 \bmod 26$	21	V
I	$(8 \times 15) + 20 \bmod 26$	10	K
S	$(18 \times 15) + 20 \bmod 26$	4	E
I	$(8 \times 15) + 20 \bmod 26$	10	K
S	$(18 \times 15) + 20 \bmod 26$	4	E
A	$(0 \times 15) + 20 \bmod 26$	20	U
N	$(13 \times 15) + 20 \bmod 26$	7	H
E	$(4 \times 15) + 20 \bmod 26$	2	C
X	$(23 \times 15) + 20 \bmod 26$	1	B
E	$(4 \times 15) + 20 \bmod 26$	2	C
R	$(17 \times 15) + 20 \bmod 26$	15	P
C	$(2 \times 15) + 20 \bmod 26$	24	Y
I	$(8 \times 15) + 20 \bmod 26$	10	K
S	$(18 \times 15) + 20 \bmod 26$	4	E
E	$(4 \times 15) + 20 \bmod 26$	2	C

cipher text :- TVKEKEUHCBCPYKEC.

KAHKASHA KHAN
15BCS013

Date ___/___/___

Q-9. Let the possible key be :- 11, 12, 13, 14, 15, ~~16~~.

case-1 : key = 11.

N	(13-11) mod 26	2	c
C	(2-11) mod 26	17	r
J	(9-11) mod 26	24	y
A	(0-11) mod 26	15	p
F	(4-11) mod 26	19	t
Z	(25-11) mod 26	14	o
B	(17-11) mod 26	6	g
C			r
L	(11-11) mod 26	0	a
A			p
S	(18-11) mod 26	7	h
J			y
L			a
Y	(24-11) mod 26	13	n
O	(14-11) mod 26	3	d
D	(3-11) mod 26	18	s
F			t
P	(15-11) mod 26	4	e
R			g
L			a
Y			n
Z			o
R			g
C			r
L			a
A			p

Page No.

KAHKASHA KHAN
15BCS013

S			h
J			y
L			a
C			u
P			e
E			+
H	(7-11) mod 26	22	w
X			o
D			s
T	(19-11) mod 26	8	i
O			d
P			e
D			s
X			o
Q	(16-11) mod 26	5	f
L			a
N	(13-11) mod 26.	2	6
Z			0
T			a i
Y			n.

plain text : cryptography & steganography are two sides of a coin

KAHKASHA KHAN
19BCS013

Date ___/___/___

Q-10. The length of the message is 12. The size of the block needs to divide 12.

This means that the size of the block can be 1, 2, 3, 4, 6, 12.

Since 1 & 12 are trivial we can ignore them.

If size of the matrix is 4 or 6 we need at least the plaintext / ciphertext of size 16 or 36. Hence these are not possible.

Hence our only choices are 2 & 3.

Let's try for 2 :—

$$P = \begin{bmatrix} 11 & 04 \\ 19 & 20 \end{bmatrix} \qquad C = \begin{bmatrix} 07 & 01 \\ 02 & 03 \end{bmatrix}$$

Since P is not invertible, module 26. we cannot proceed.

Let try for size 3 :—

$$P = \begin{bmatrix} 11 & 04 & 19 \\ 20 & 18 & 12 \\ 04 & 04 & 19 \end{bmatrix} \qquad C = \begin{bmatrix} 07 & 01 & 02 \\ 03 & 05 & 13 \\ 14 & 15 & 08 \end{bmatrix}$$

KAHKASHA KHAN
19BCS013

Date ___/___/___

since, p is not invertible in modulo 26. Hence, we can't proceed.

This means that we cannot solve the problem with the information given.

Q-11 When eve tabulates the frequency of letters in this ciphertext, she gets :-

I = 14, V = 13, S = 12 & so on.

The most common character is S with 14 occurrences

This means key = 4 (e, f, g, h, i)

Plain text :-
The house is now ~~sale~~ for sale for four million dollars, it is worth more hurry before the seller recieves more offers.