COMPUTER ENGINEERING DEPARTMENT

PRACTICE TEST

SUB: CSS

COURSE: T.E. **Year: 2020-2021** **Semester: VI**

DEPT: Computer Engineering

SUBJECT CODE: CSC604 **SUBMISSION DATE: 14/05/2021**

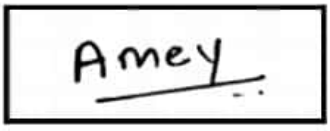
==========

Name: Amey Thakur **Roll No.: 50**

Class: TE Comps B-50 **ID: TU3F1819127**

PRACTICE TEST

Sr. No.	Question (Solve any 5)
1	Explain the following Symmetric cipher methods: Playfair cipher, vigenere cipher, hill cipher.
2	What is the purpose of the S-boxes in DES? Discuss the design details of s-box.
3	Explain the various ways to calculate Modular Multiplicative Inverse: Extended Euclidean Algorithm, Fermat's Theorem, Euler's Theorem.
4	Define Kerberos and name its servers. Briefly explain the duties of each.
5	Explain the following targeted malicious attack: Trojan, trapdoor, backdoor, rootkit, salami attack, a man in the middle, covert channel.
6	Explain different types of firewalls.
7	Describe SSL with its types.
8	Which services are provided by IPSec?



AMEY B 50 Amey

Q1 Playfair Cipher:

It is multiple letter encryption technique which uses 5 * 5 marine table to store the letters of the phrase given for encryption which letter on becomes key for encryption and decryption. eg. Keyword is FAIR EXAMPLE

Hill Cipher:

- It is a polygraphic substitution cipher based on Linear Algebra.
- Each letter is represented by a number modulo 26. Often the simple scheme (A = 0, B = 1, C = 2, ..., Z = 25) is used, but this is not an essential feature of the cipher.
- To encrypt a plaintext message, each block is multiplied by an invertible m * m matrix, each block is multiplied by the inverse of the matrix used for encryption.

AMEY TE B 50 Amey

PAGE No.
DATE / /

The technique can be described as following:

$$C_{i1} = (K_{11} P_{i1} + K_{12} P_{i2} + K_{13} P_{i3}) \bmod 26$$
$$C_{i2} = (K_{21} P_{i1} + K_{22} P_{i2} + K_{23} P_{i3}) \bmod 26$$
$$C_{i3} = (K_{31} P_{i1} + K_{32} P_{i2} + K_{33} P_{i3}) \bmod 26$$

This technique uses column vector and matrices:

$$\begin{bmatrix} C_{i1} \\ C_{i2} \\ C_{i3} \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_{i1} \\ P_{i2} \\ P_{i3} \end{bmatrix} \bmod 26$$

Example: Encrypt the message "Exam" using the Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Solution: Key $(K) = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Plaintext (P_i) = "Exam"

$$C_i = KP_i \bmod 26 \quad \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 4 & 23 \\ 0 & 12 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 151 & 167 \\ 60 & 84 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 & 11 \\ 8 & 6 \end{bmatrix}$$

$$= VLIG$$

AMEY TE B 50 Amey

PAGE No. / DATE / /

Vigenere Cipher :

This is a method of encryption alphabetic text. It uses a simple form of polyalphabetic.

- A polyalphabetic cipher is any cipher based on substitution using multiple substition alphabets. The encryption of the original text is done using the vigenere square or vigenere table.
- The table consists of the alphabet written out 26 times in different rows, each alphabets shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caeser Ciphers.
- At different points in the encryption process the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Formula of encryption :

$$E_i = (P_i + K_i) \bmod 26$$

Formula of decryption :

$$D_i = (E_i - K_i) \bmod 26$$

where, E ⇒ Encryption
D ⇒ Decryption
P ⇒ Plaintext
K ⇒ Key

AMEY TE B 50 Amey

PAGE No.
DATE / /

A	00
B	01
C	02
D	03
E	04
F	05
G	06
H	07
I	08
J	09
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Example:

Plaintext = AMEY
KEY = MEGA

Plaintext	A	M	E	Y
Value (P)	00	12	04	24
Key	M	E	G	A
Value (K)	12	04	06	00
Ciphertext Value(E)	12	16	10	24
Ciphertext	M	Q	K	Y

Ciphertext (E)	M	Q	K	Y
	12	16	10	24
key (K)	M	E	G	A
	12	04	06	00
(P)	00	12	04	24
Plaintext	A	M	E	Y

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q3. Explain the Euclid Algorithm, Fermat / Euler Algorithm.

Ans:

Euclid Algorithm:

- The Euclidean algorithm is a technique for quickly finding the GCD of two integer.
- The Eucladean algorithm for finding out GCD (A, B) is as follows:
- If A = 0 then GCD (A, B) = B.
  ∵ GCD (0, B) = B and we can stop.
- If B = 0 then GCD (A, B) = A.
  ∵ GCD (A, 0) = A and we can stop.
- Write A in qotient remainder form
  (A = B · Q + B)
- Find GCD (B, R) using the Euclidean algorithm since GCD (A, B) = GCD (B, R)

Example : Find the GCD of 270 & 192

A = 270 A ≠ 0

B = 192 B ≠ 0

Use long division to find that 270/192 = 1 with a remainder of 78.

270 = 192 * 1 + 78

Find GCD (192, 78) since GCD (270, 192) = GCD (192, 78)

A = 192 B = 78

A ≠ 0 B ≠ 0

AMEY TE B 50 Amey

PAGE No.
DATE / /

Use long division to find that 192/78 = 2 with a remainder of 36.

192 = 78 * 2 + 36

Find GCD (192, 78) since GCD(192, 78) = GCD(78, 36)

A = 78 A ≠ 0
B = 36 B ≠ 0

Use long division to find that 78/36 = 2 with a remainder of 6.
We can write this as:
78 = 36 * 2 + 6

Find GCD (36, 6), since GCD(78, 36) = GCD(36, 6)

A = 36 A ≠ 0
B = 6 B ≠ 0

Use long division to find that 36/6 = 6 with a remainder of 0.

36 = 6 * 6 + 0

Find GCD(6, 0), since GCD(36, 6) = GCD(6, 0).

A = 6 A ≠ 0
B = 0 B = 0 GCD(6, 0) = 6

AMEY TE B 50 Amey

PAGE No.
DATE / /

GCD (270, 192)
= GCD (192, 78)
= GCD (78, 36)
= GCD (36, 6)
= GCD (6, 0)
= 6

∴ GCD (270, 192) = 6

Euler's Theorem:

It states that for every a & n that are relatively prime:

$$a^{\phi(n)} = 1 \pmod{n}$$

Example:

a = 3
n = 10
$\phi(n)$ = ?

Let $\phi(n) = \phi(10) = \{1, 3, 7, 9\} = 4$

According to Euler's Theorem.

$3^4 = 1 \pmod{10}$
$3^4 = 1 \mod 10$
$81 = 1 \mod 10$ (81 mod 10
= 1 ∠ 1 mod 10
= 1)

Hence Proved

AMEY TE B 50 Amey

PAGE No. DATE / /

Fermat Theorem

Fermat Theorem plays an important role in public key cryptography.

Theorem:

- For a prime number p, a is an integer which is not divisible by p then,

$$a^{p-1} \pmod{p}$$

A variant of this theorem is

If p is a prime and a is a coprime to (i.e GCD (a, p) = 1) then,

$$a^p \equiv a \pmod{p}$$

- Basically this theorem is useful in public key RSA and primarily testing
- Let us have $a = 3$ & $p = 5$. then as per the above theorem we have $3^{5-1} = 3^4 = 81 = 1 \pmod{5}$

Since, on dividing 81 with 5, we have remainder 1.

Hence Proved

AMEY B 50 Amey

Q4. Needham Schroeder / Kerberos Authentication

- Kerberos infrastructure relies on Needham Schroeder Protocol.
- Needham Schroeder protocol refers to a communication protocol used to secure an insecure network. The protocol got its name from the creators Roger Needham and Michael Schroeder.
- There are two types of Needham - Schroeder protocol.
  1. Needham - Schroeder protocol with symmetric key
  2. Needham - Schroeder protocol with Asymmetric key

AMEY TE B 50 Amey

PAGE No.
DATE / /

- Now lets understand Needham - Schroeder protocol with symmetric key encryption because its the one used in Kerberos infrastructure.

- Needham - Schroeder protocol allows to prove the identity of the end users communicating, and also prevents a middle man from evesdropping.

- We will be using some terms

Nonce :

- Nonce is a randomly generated string which is only valid for some period of time. This is used in encryption protocol to prevent replay attack
- For example, if somebody captures a packet during the communication between me and a shopping website, he can resend the packet without decrypting it, and the server can accept the packet and do operations on it. To prevent this, nonce (the random value generated) is added to the data, so as the server can check if that nonce is valid or expired.

- Lets understand this protocol by taking an example communication between two machines called Machine A and Machine B.

- The main thing in this protocol is that there is a trusted middle man or call him an arbitrator. This trusted middle man is a server. If an X machine wants to communicate with Y machine. Then X has to contact the middle man server saying am interested in communicating with Y.

AMEY TE B 50 Amey

PAGE NO.
DATE / /

Lets see how it works.

A = Machine A

B = Machine B

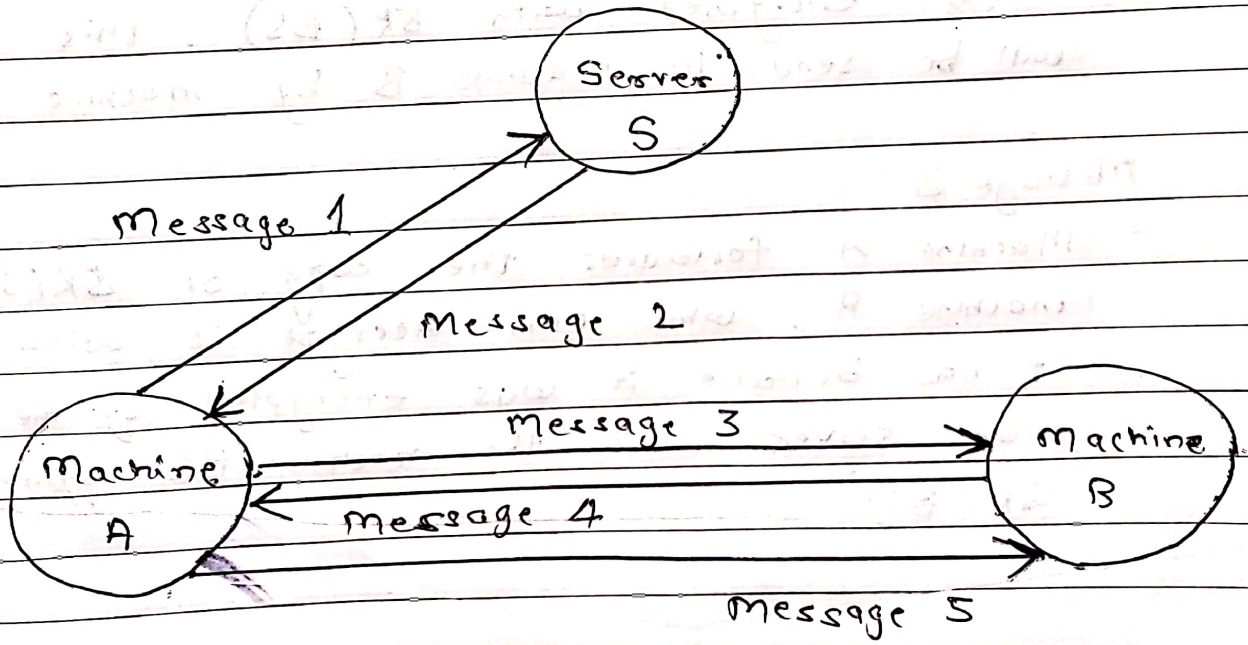
SK (AS) = This is the symmetric key known to machine A and middle man Server named S.

SK (BS) = This is the symmetric key known to machine B and middle man Server named S.

NOW (A) = Nonce generated by Machine A.

NON (B) = Nonce generated by Machine B.

SK (S) = This is the symmetric key/ session key generated by the server for both machine A and machine B.



AMEY TE B 50 Amey PAGE No. DATE / /

- Lets understand all the messages mentioned above.

- Initially before going ahead with the explanation, make it clear that the symmetric keys of both machine A, machine B are already shared with the middle man server. Also any other machine in the network also shares its respective symmetric keys with the middle man server.

Message 1:

- Machine 1 sends a message to server S saying that I want to communicate with machine B.

- A → S (This message contains A and B and NON(A))

Message 2:

- Server S sends message 2 back to machine A containing SK(S), and also one more copy of SK(S) encrypted with SK(BS). this copy will be send to machine B by machine A.

Message 3:

- Machine A forwards the copy of SK(S) to machine B, who can decrypt it with the key it has because it was encrypted by the middle man server with the machine B's symmetric key SK(BS).

AMEY TE B 50

Amey

PAGE No.
DATE / /

Message 4:

- Machine B sends back machine A a nonce value encrypted by SK(S) to confirm that he has the symmetric key or session key provided by the middle man server.

Message 5:

- Machine A performs a simple operation on the nonce provided by the Machine B and resends that back to machine B just to verify machine A has the key.

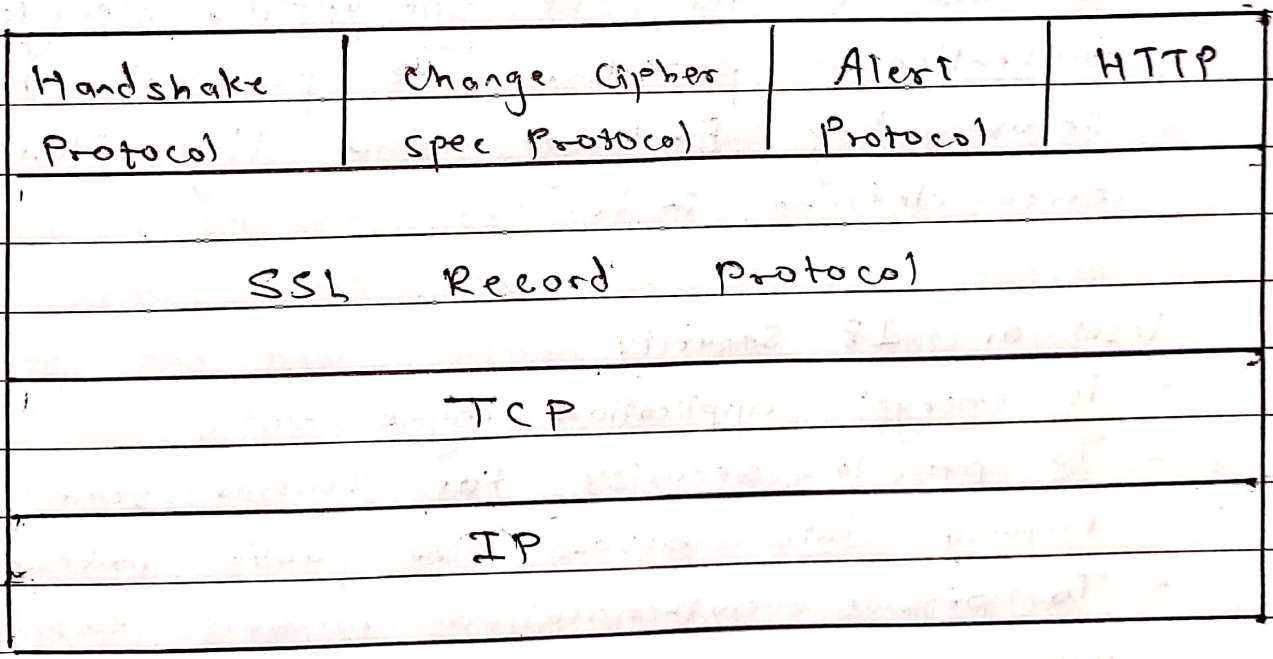
- There are still some vulnerabilities in this protocol for replay attacks which is fixed by the timestamp implementation in this, when used by Kerberos.

Amey PAGE No. 1 DATE / /

Q.7 Explain

SSL

- Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack
- Secure Socket Layer Protocols
  1. SSL record protocol
  2. Handshake protocol
  3. Change - cipher spec protocol
  4. Alert protocol
- SSL protocol stack



- SSL Record provide two services to SSL connection
  1. Confidentiality
  2. Message Integrity

AMEY TE B -50 Amey

PAGE No.
DATE / /

Features of SSL

- Advantage of this approach is that the service can be tailored to the specific needs of the given application
- Secure Socket Layer was originated by Netscape
- SSL is designed to make use of TCP to provide reliable end to end secure service
- This is a two layered protocol

AMEY B 50 Amey

Q8 IPSec

- The IP Security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provides data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key Exchange and Key Management are defined in it.

Uses of IP Security

- To encrypt application layer data
- To provide security for routers sending sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPSec tunneling in which all data is being sent between the two endpoints is encrypted as with a Virtual Private Network (VPN) connection.

AMEY TE B 50

Components of IPsec

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)