COMPUTER ENGINEERING DEPARTMENT

SUBJECT: CRYPTOGRAPHY & SYSTEM SECURITY

COURSE: T.E. **YEAR: 2020-2021** **SEMESTER: VI**
DEPT: COMPUTER ENGINEERING
SUBJECT CODE: CSC604 **EXAMINATION DATE: 09/06/2021**

==========

CRYPTOGRAPHY & SYSTEM SECURITY
ANSWER SHEET

NAME : AMEY MAHENDRA THAKUR

SEAT NO. : 61021145

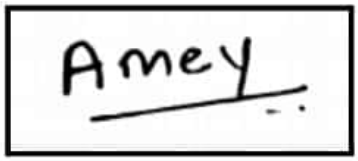
EXAM : SEMESTER VI

SUBJECT : CRYPTOGRAPHY & SYSTEM SECURITY

DATE : 09-06-2021

DAY : WEDNESDAY

STUDENT SIGNATURE:



Q2

A]

Security Goals / Security services

- Providing security to the information assets of our modern age has become a matter of supreme importance.
- The three main goals associated with security are:
  1. Confidentiality
  2. Integrity
  3. Availability

① Confidentiality:

- It is a common aspect of information security. We need to protect our confidential information from getting leaked into public.
- For example, in military, confidentiality is related to national security. In business, certain information always needs to be hidden from competitors.
- It applies to both the storage of information as well as for transmission of information.

② Integrity:

- In information security, integrity means maintaining and assuring accuracy and completion of data over its entire life cycle.
- It means that changes can be done only by authorized entities and only through authorized mechanism.
- Security integrity of data is extremely important.

Eg. You are sending Rs 1000, Somebody tampers with the integrity of transaction and actually sends Rs 100000.

09-06-2021

STUDENT SIGNATURE: Amey

③ Availability:
- Availability of information refess to ensuring that authorized entities get information when needed.
- An information which is stored and maintained is useless if it's not available when needed.
- Denying access to the information has become a popular mode of cyberattack.
Example: DDOS (Distributed Denial of Service).

Mechanisms to achieve above goals are:

① Confidentiality → Encipherment
→ Routing Control.

② Integrity → Encipherment
→ Digital Signature
→ Data Integrity

③ Availability → Creating backups
→ Routing Control

09 - 06 - 2021 STUDENT SIGNATURE: Amey

Security Mechanisms.

① Encipherment:
- This is hiding or covering of data which provides confidentiality.
- Cryptography and Steganography are used in encipherment.

② Digital Integrity.
- The data integrity mechanism appends a short check value to the data that has been created by a specific process from the data itself.

③ Digital signature
- A digital signature is a means by which the sender can electronically sign the data and receiver can electonically verify the signature.

④ Authentication Exchange
- In this two entities exchange some message to prove their identity to each other.

⑤ Traffic Padding
- Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

09-06-2021

STUDENT SIGNATURE: Amey

⑥ Routing (control):
- Routing control means selecting and continuously changing different available routes between sender and receiver to prevent eavesdropping.

⑦ Access Control.
- Access control method to prove that a user has access right to the data or resource owned by system.

09-06-2021

STUDENT SIGNATURE: Amey

Q2

B] Diffie Hellman

Diffie Hellman Key Exchange Algorithm:

- The Diffie Hellman algorithm was widely known as Key exchange algorithm or key aggrement algorithm developed by Whitfield Diffie and Martin Hellman in 1976
- Diffie Hellman algorithm is used to generate same (symmetric) private cryptographic key at sender as well as receiver end so that there is no need to transfer this key from sender to receiver.
- Remember that Diffie Hellman algorithm is used only for key aggrement not for encryption or decryption of message.
- If sender and receiver want to communicate with each other they first agree on the same key generated by Diffie Hellman algorithm later on they can use this key for encryption or decryption.

09-06-2021 STUDENT SIGNATURE: Amey

Steps of Diffie Hellman Algorithm

1. The first step is that if Ramesh wants to communicate with Suresh they must agree on two large prime numbers p and q.
2. Ramesh selects another secret large random integer a, and calculate R such that $R = q^a \bmod p$.
3. Ramesh sends this R to Suresh
4. Suresh independently selects another secret large random integer b, Calculate S such that.
   $S = q^b \bmod p$
5. Suresh sends the number S to Ramesh
6. Now Ramesh is calculating his secret key by using $R_K = S^a \bmod p$.
7. Suresh is calculating his secret key S_K by using $S_K = R^b \bmod p$.
8. If $R_K = S_K$ then Ramesh and Suresh can agree for future communication called as Key Aggrement Algorithm.
9. We have $R_K = S_K = K$. (K is symmetric key).

Hence Proved.

09-06-2021

STUDENT SIGNATURE: Amey

For Example :

(1) Ramesh and Suresh are agree on two large prime numbers say $p = 17$ and $q = 7$.

(2) Ramesh selects another secret large random number 5 i.e. $a = 5$ and calculate R such that.

$$R = q^a \bmod p = 7^5 \bmod 17 = 11$$
$$= (7 \times 7 \times 7 \times 7 \times 7) \bmod 17 = 11$$

(3) Ramesh sends R to Suresh.

(4) Suresh selects another secret large random number 3. i.e. $b = 3$ and calculate S such that.

$$S = q^b \bmod p = 7^3 \bmod 17 = 3$$
$$= (7 \times 7 \times 7) \bmod 17 = 3$$

(5) Suresh sends numbers S to Ramesh.

(6) Ramesh now calculates its secret key R_K

$$R_K = S^a \bmod p = S^5 \bmod 17$$
$$\therefore R_K = 3^5 \bmod 17 = 5$$
$$= (3 \times 3 \times 3 \times 3 \times 3) \bmod 17 = 5.$$

(7) Suresh is calculating its secret key S_K

$$S_K = R^b \bmod p = R^3 \bmod 17$$
$$= 11^3 \bmod 17$$
$$= 5$$

(8) If $R_K = S_K$ then Ramesh and Suresh can agree for future future communication.

(9) We know that if $R_K = S_K = X = 5$.

Hence Proved.

09-06-2021 STUDENT SIGNATURE: Amey

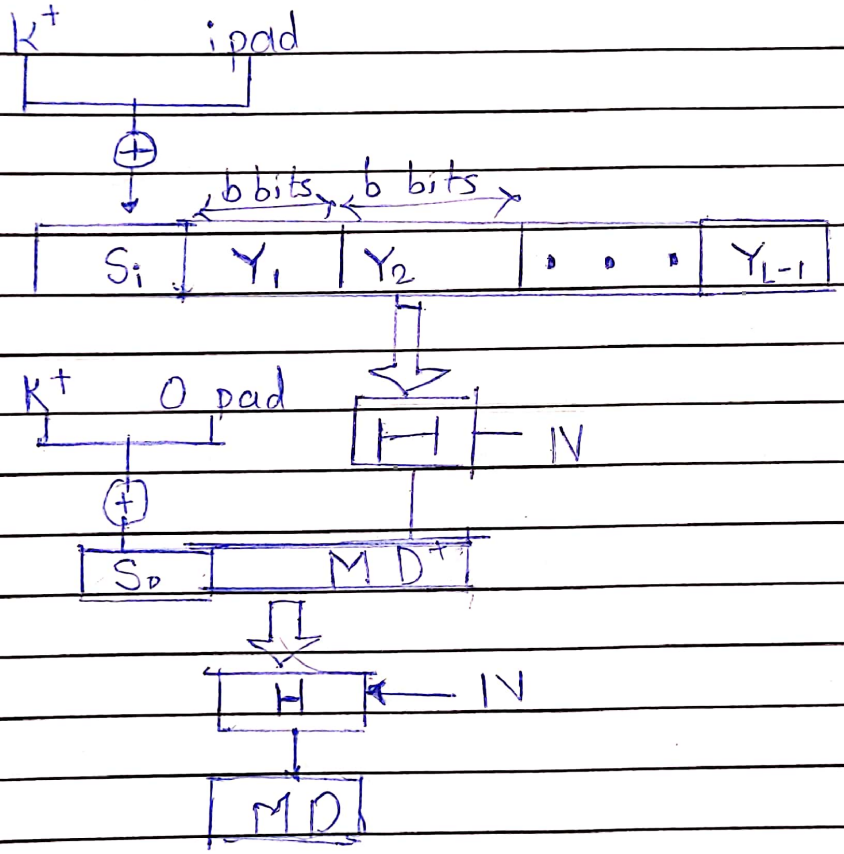
Q2.

C] HMAC

HMAC

- Hash Based Message Authentication Code (HMAC) is a message authentication code that uses a cryptographic key in conjunction with a hash function.

HMAC Algorithm:



09-06-2021

STUDENT SIGNATURE: Amey

Here H stands for Hashing function.
M is original message
Si and So are input and output signatures
Yi is the ith block in original message M.
i ranges from [1, L).

L = Count of block in M
K is the secret key used in Hashing
IV is an initial vector (some constant).
The generation of input Si and output So

$S_i = K^+ \oplus ipad$

$S_o = K^+ \oplus opad$

$M_D' = H(S_i \| M)$

$MD = H(S_o \| MD')$

Comment on HMAC Security:
- HMAC is a great resistant towards cryptanaly sis attack as it uses the hashing concept twice.
- HMAC consists of twin benefits of Hashing and MAC. and thus it is more secure than any other authentication codes

09-06-2021

STUDENT SIGNATURE: Amey