ID- 2017140 18
Ayon Roy

CT-02

CSE-429

Roll : 2017140 18

CSE-17

Sec: B

Ayan Roy

Ans. to the ques. no.-01(a)

For the MCAM system of MIST security services and mechanisms are as follows:

a) Authentication
b) Access control
c) Data Confidentiality
d) Data Integrity
e) Non repudiation.

a) Authentication: No student or teacher can see other students or teachers contents of MCAM (CT marks, Mid marks, attendance etc)

b) Access control: MCAM should only be accessed by personal pc and smartphones and the database should only be accessed by the MCAM website.

P.T.O →

2017140018

Ayesha

c) Data confidentiality: Data in the MCAM should be private so that anyone can not see the data. privacy should also be maintained.

d) Data Integrity: Data in MCAM should change through authorized process and should maintain integrity.

e) Non repudiation: This involves no student can say they were present and no teacher can say they didn't give Attendance while MCAM suggests otherwise.

Some steps to improve security of the system are given below:

ⓐ Encrypt data with higher key value.

ⓑ Using public and private key encryption.

P.T.O.

20171401B

Ayesha

(c) No access to site without Login first (authentication).

(d) Ensure Authorization.

(e) Log every action taken in MCAM.

(f) Backup data.

(g) Deploy firewalls in the Network and Resources Level.

(h) Separate UI interfaces for Admin and (Student & Teachers).

P.T.O.

2017140018

Sayeef

Ans. to the ques. no. - 01(b)

Cryptography is the process where we convert text from ~~one~~ ~~into~~ one form to another using algorithms and keys.

Steganography is the process where hide the original message inside another message or inside an RGB Image.

My suggestion to combine the both to make a more secure hybrid system are given below:

① First encrypt the message using additive or multiplicative cipher with a key K. (this time we use symetric cipher, only one key for sender and receiver).

P.T.O.

2017140018

Ayshey

② To use additive cypher with key k ~~to~~ first, ~~convert the~~ map all alphabets in the language to numbers (0 to 25).

then, use the following algo for all alphabets:

$C_1 = (P + k) \bmod 26$.

③ Then we use the multiplicative cypher with the ciphertext(C_1) we get at (step-2). and get ciphertext-2 (C_2)

$C_2 = (C_1 * k) \bmod 26$.

④ Then we use steganography inside an RGB image to ~~to~~ hide the ciphertext-2 (C_2).

If C_2 becomes: 2 3 4 5 6...

Then the image would be

Pixels →	R	G	B
	242 ~~2~~ 2	230 ~~4~~ 3	2 ~~2~~ 0 – 5
↘	210 – 6	...	...

P.T.O

2017140018

Hiding the ciphertext inside the image will gurantee security.

To get the original text steps;

① get cipher from the image (RGB) RGB values will get that. (C_2)

② Use algo to get C_1.

$$C_1 = (C_2 \times K^{-1}) \bmod 26$$

③ Use algo to get plaintext.

$$P = (C_1 - K) \bmod 26.$$

T.T.O.

2017140188

Ans. to the ques. no - 01(c)

Polyalphabetic substitution is equivalent to multiple mono-alphabetic substitution.

Polyalphabetic substitution is where the original each character can have a list of homophones to map to. the plaintext and ciphertext have relationship of one-to-many.

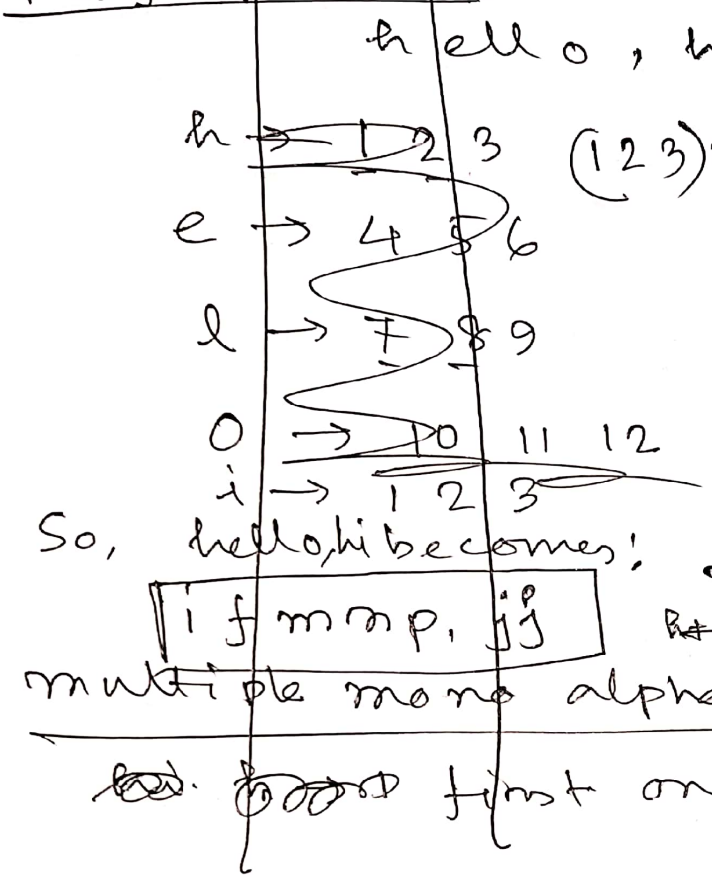
multiple mono-alphabetic substitution is when original character is substituted to another character multiple times using multiple keys..

Both polyalphabetic and multialphabet

P.T.O

has one-to-many relationship.
both have multiple mapping of original to final ciphertext.

An Example:
Poly alphabetic:



So, hello,hi becomes: ~~iist, jj~~
ifmmp, jj ~~h+1=i, e+4=i~~

multiple mono alphabetic: for hello,
~~first~~ first one.

getting multiple mappings in poly alphabetic or getting multiple mapping in different steps in mono-alphabetic are equivalent. hello → (Poly alpha) iist ↔ same. hello → (mono) iist