CSS
Assignment 1

8875
Upmanya Jha
Comps A

1.Q solution] i) Confidentiality : This element is the protection of data from unauthorized access and misuse. Organisations will always have some form of sensitive data stored on their systems. To provide confidentiality is to protect this data from parties that it is not intended for.

Ex.

Employee records and accounting documents will be considered sensitive. Confidentiality will be provided in the sense that only HR administrators will access employee records, where Vetting and right access controls are in place. Accounting records are less valuable, so not as stringent access controls would be in place for these documents. Or, for example, governments using a sensitivity classification rating system (top-secret, classified, unclassified)

Integrity :- The CIA triad element of integrity is the condition where information is kept accurate and consistent unless authorized changes are made. It is possible for the information to change because of careless access and use, errors in the information system, or unauthorized access and use. In the CIA triad, integrity is maintained when the information remains unchanged during storage, transmission, and usage not involving modification to the information. Steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Non - repudiation: It is basically an ability of a person to approve or disapprove something.

Real life example: (a) forensic labs

(b) IP address

(c) Email.

Suitable security mechanism to achieve this is email tracking.

Q2 solution.] With the keyword in a matrix, we need to convert this into a key matrix. We do this by converting each letter into a number by its position in the alphabets (starting at 0)

In short treat every letter in the plain text message as a no., so that A = 0, B = 1 ... Z = 25

The keyword written as a matrix "Hill"

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

The key matrix to each letter of the keyword is converted to no.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

Now we split the plaintext into digraphs and write them as column vectors. That is in the first col. vector we first plaintext letter at the top and second at bottom and so on

for the word "short",

Hill requires bigraphs (pair of plaintext) to process

∴ it would be split as

$\begin{pmatrix} S \\ L \end{pmatrix} \begin{pmatrix} O \\ Y \end{pmatrix} \begin{pmatrix} T \\ X \end{pmatrix}$ → {ord letter of keyboard converted to no. }

$\begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 23 \end{pmatrix}$

Matrix multiplication of keyword "HILL" and first pair of plaintext

i.e $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \end{pmatrix}$

$7 \times 18 + 8 \times 7 = 182$

$11 \times 18 + 11 \times 7 = 275$

$\therefore \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} A \\ P \end{pmatrix}$

$\therefore \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} S \\ H \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} = \begin{pmatrix} 0 \\ 10 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} A \\ P \end{pmatrix}$

Similarly for next pair

$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} A \\ D \end{pmatrix}$

$7 \times 14 + 8 \times 17 = 234$

$11 \times 14 + 11 \times 17 = 341$

Similarly for next pair (L, X)

$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 23 \end{pmatrix} = \begin{pmatrix} 317 \\ 462 \end{pmatrix} = \begin{pmatrix} 5 \\ 20 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} F \\ U \end{pmatrix}$

$7 \times 19 + 8 \times 23 = 317$

$11 \times 19 + 11 \times 23 = 462$

$\therefore$ The final ciphertext for the plaintext "SHORT" is "APADFU".

Short questions:

1 Ans. Purpose of Diffie Hellman key exchange:

a) Encryption: The Diffie Hellman key exchange algorithm can be used to encrypt one of the first schemes to do is ElGamal Encryption. One modern example of it is called Integrated Encryption Scheme, which provides security against chosen plaintext and chosen ciphertext attacks.

b) Password Authenticated Agreement: When two parties share a password / a password ~~authentication~~ authenticated key agreement can be used to prevent the Man in the middle attack. This key Agreement can be in the form of Diffie Hellman. Secure Remote Protocol is good example that is based on this technique.

(c) Forward Secrecy: Forward secrecy based protocols can generate new key pairs for each new session and then they automatically discard them when the session is finished.

In these secrecy protocols, more often than not, the Diffie Hellman key exchange is used.

⇒ Diffie Hellman is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. This key can be used to encrypt subsequent communication using a symmetric key cipher. Diffe Hellman Algorithm is used to generate public key. Public key for key exchange allows 2 users to exchange

(1) Ans

→ By Fermat's theorem

$$a^{p-1} \equiv 1 \bmod p$$

given $3^4 \bmod 11$

Here $a = 3$, p (is a prime no.) $= 11$,

$(p-1) = (11-1) = 10$

∴ By Fermats theorem

$$3^{10} \equiv 1 \bmod 11$$

$$\therefore 3^{10} \bmod 11 = 1 \quad \text{---(2)}$$

given,

$3^4 \bmod 11$

$(3^{(10*2+1)}) \bmod 11 = (3^{10})^2 \cdot 3^1 \bmod 11$

$= (3^6)^2 \bmod 11 \times 3^1 \bmod 11 = 1 \times 3^1 \bmod 11$ (from 2)

$= 3 \bmod 11$

$= 3$

A.