NAME :- KRUNAL RANK

ROLL NO :- U18CO081

CLASS :- BTECH 4TH YEAR

SEMESTER :- 7

DIVISION :- B

Cryptography and Network Security
Tutorial 4

Ans 1:-

Confusion	Diffusion
• Confusion is a cryptographic technique which is used to create faint cipher texts.	• Diffusion is used to create cryptic plain texts.
• The technique is possible through substitution techniques.	• The technique is possible through transposition or permutation techniques.
• In confusion, if one bit within the secret is modified, most or all bits in cipher text will be modified.	• In diffusion, if one part of plain text is modified, many or all images in cipher text will be modified.
• Vagueness is increased.	• Redundancy of plaintext is increased.
• Example:- Stream cipher, Caesar Cipher.	• Example:- Railfence cipher

Ans 2:- The two major problems with one time pad are as follows:-

- The secret needs to be of the same length ~~as~~ to that of the message which is ~~problema~~ problematic for large messages.
- Everytime a message is transmitted, a new one time pad needs to be generated and shared with the receiver well in advanced in a secure manner that makes this protocol practically illogical.

Ans3. Some modes of operations work in such a way that only known values are ever encrypted, forming a stream of pseudo random data that is then combined with the plaintext by a keyless reversible operation (often xor) to form the ciphertext.

Other modes directly encrypt secret values meaning decryption is required to find out what the secret value is.

Ans4. In one time pad technique, a key equal to the length of plain text needs to be generated every time ~~a transmi~~ encryption is carried out.
On the other stream cipher technique uses a key of fixed length to create a unique key equal to the length ~~o~~ of plain text to then carry out the encryption process.

One time pad is an impractical method but provides perfect secracy.
Stream cipher compromises with perfect secracy to provide a method that is feasible and semantically secret.

Ans5. ~~The One tim~~

Cipher text :- TICRMQUIRTJR
Plain text :- CRYPTOGRAPHY

Possible Key :- RRECTCORRECT
Hence, it is seen that the key is actually repetition of the word CORRECT

Ans 6:- The one time pad achieves perfect secracy which can be justified as follows:-

- It comprises a sequence of random symbols drawn from the aphabets as the message which is known both to the sender and receiver.
- A message is encrypted by combining it with the respective segment of the sequence having the same length as the message.
- The segment is then discarded.
- The segment is the key and in case of message made up of bits combinining of the message and the key can be as simple as XORing the two sequences.
- Hence, even if the attacker somehow decrypts some part of the cipher text, he/she gets no clue about any other part of the cipher text, thereby making one time pad achieving perfect secracy.

Ans 7:- Given text:- "MEETMEATTHEUSUALPLACEATTENRATHERTHAN EIGHTOCLOCK

Pairing the text characters, we get,

ME ET ME AT TH EU SU AL PL AC EA TT EN

RA TH ER TH AN EI GH TO CL OC KZ

Now encryption of ME is given by :-

$$\begin{pmatrix}9 & 4\\5 & 7\end{pmatrix}'\begin{pmatrix}12\\4\end{pmatrix} = \begin{pmatrix}128\\88\end{pmatrix} \% 26 + 1 = \begin{pmatrix}20\\10\end{pmatrix} = \begin{pmatrix}U\\K\end{pmatrix}$$

Hence, in a similar fashion, we get,

cipher text = "UKIXUKYDROMEIWS ZXWIOKUNUKHXROA
JROANQYEBTLKJEGM"

To find ~~its~~ the inverse key, we need to find inverse matrix for the given key :-

$$~~|A|~~ \; |Key| = 9\times7 - 5\times4 = 43$$

$$\text{Inverse} = \frac{1}{|Key|}\text{Adj}(Key) = \begin{pmatrix}7 & -4\\-5 & 9\end{pmatrix}\times\frac{1}{43} = \frac{1}{17}\begin{pmatrix}7 & -4\\-5 & 9\end{pmatrix} \quad \{\because 43 \% 26 = 17\}$$

Mod Inverse of 17 = 23

$$\text{Hence, Inverse Key} = \begin{pmatrix}161 & -92\\-115 & 207\end{pmatrix} \% 26 = \begin{pmatrix}5 & -14\\-11 & 25\end{pmatrix}$$

$$= \underline{\begin{pmatrix}5 & 12\\15 & 25\end{pmatrix}}$$