Name : Sradha Kedia
Date of Examination : 18 December, 2021
Time of Examination : 9:30 am to 1:30 pm
Examination Roll no : 20234757053
Semester : III
Unique Paper Code : 22340302
Title of Paper : Information Security
Email-Id : 200083@cs.du.ac.in
Mobile no of student : ~~200083@cs.du.ac.in~~ 9899519848
Question no : 5
No. of pages : 4
Name of the program : MCA
Name of the Department : DUCS

Ans 5(ii) Differentiate Assymetric and symmetric cryptography.

Symmetric Key Cryptography	Assymetric Cryptography
• Only Requires one single key for encryption and decryption	• It requires 2 keys one to encrypt, another to decrypt.
• Encryption is fast • This technique provides only confidentiality	• Encryption is slow. • This provides confidentiality authenticity and non-repudiation.
• best fit to transfer large amount of data.	• to transfer small amount of data.
• eg- DES, RC4, AES	• eg- RSA, Diffie Hillman DSA.

These two techniques can be combined to make a more secure cryptosystem which is called as hybrid encryption.
As symmetric cryptography is best suited to encrypt large amount of data, we use it to encrypt the text, where recipient public key can be used to encrypt symmetric key only. The result will be symmetric ciphertext and the encrypted symmetric key that can be decrypted only by reciever's private key.

i) a) In CFB mode, the key generator for block i uses C_{i-1}, the ciphertext created in block i-1; Acc. to definition of non synchronous stream cipher, the key stream is somehow dependent on the plaintext or ciphertext.
While in synchronous ciphers, the key stream is independent of plaintext or ciphertext that means In OFB mode, the key generator for block i uses part of the key from previous block, but it is independent from plaintext and ciphertext in previous block so OFB is an synchronous cipher.

b) In CFB, OFB, and CRT; are stream ciphers; the size of block is usually fixed (one character) there is no need of padding. This means there is no need for cipher stealing technique it is only used when ciphertext is not XOR of plaintext and some pseudo random stream.

ii) Hill cipher :

UNIVERSITYOFDELHI

$$A = \begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26

we will take two-two characters and multiply with A mod 26.

P_i: $\begin{pmatrix} U \\ N \end{pmatrix} = \begin{pmatrix} 21 \\ 14 \end{pmatrix}$ $\begin{pmatrix} T \\ Y \end{pmatrix} = \begin{pmatrix} 20 \\ 25 \end{pmatrix}$ $\begin{pmatrix} I \\ Z \end{pmatrix} = \begin{pmatrix} 9 \\ 0 \end{pmatrix}$

$\begin{pmatrix} I \\ V \end{pmatrix} = \begin{pmatrix} 9 \\ 22 \end{pmatrix}$ $\begin{pmatrix} D \\ F \end{pmatrix} = \begin{pmatrix} 15 \\ 6 \end{pmatrix}$

$\begin{pmatrix} E \\ R \end{pmatrix} = \begin{pmatrix} 5 \\ 18 \end{pmatrix}$ $\begin{pmatrix} D \\ E \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$

$\begin{pmatrix} S \\ I \end{pmatrix} = \begin{pmatrix} 19 \\ 9 \end{pmatrix}$ $\begin{pmatrix} L \\ H \end{pmatrix} = \begin{pmatrix} 12 \\ 8 \end{pmatrix}$

$C = (A \times P_i) \bmod 26$

$$C_1 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 21 \\ 14 \end{pmatrix} = \begin{pmatrix} 91 \\ 140 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 10 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 9 \\ 22 \end{pmatrix} = \begin{pmatrix} 71 \\ 172 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 \\ 16 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 5 \\ 18 \end{pmatrix} = \begin{pmatrix} 51 \\ 136 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 \\ 6 \end{pmatrix}$$

$$C_4 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 19 \\ 9 \end{pmatrix} = \begin{pmatrix} 75 \\ 101 \end{pmatrix} \bmod 26 = \begin{pmatrix} 23 \\ 23 \end{pmatrix}$$

$$C_5 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 20 \\ 25 \end{pmatrix} = \begin{pmatrix} 110 \\ 215 \end{pmatrix} \bmod 26 = \begin{pmatrix} 6 \\ 7 \end{pmatrix}$$

$$C_6 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 15 \\ 6 \end{pmatrix} = \begin{pmatrix} 57 \\ 72 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 \\ 20 \end{pmatrix}$$

$$C_7 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 22 \\ 43 \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 \\ 17 \end{pmatrix}$$

$$C_8 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 12 \\ 8 \end{pmatrix} = \begin{pmatrix} 52 \\ 80 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$$

$$C_9 = \begin{pmatrix} 3 & 2 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 9 \\ 0 \end{pmatrix} = \begin{pmatrix} 27 \\ 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 \\ 18 \end{pmatrix}$$

13	19	25	23	6	5	22	0	1
10	16	6	23	7	20	17	2	18

ciphertext will be

M J S P Y F W W F G E T V Q Z B A R