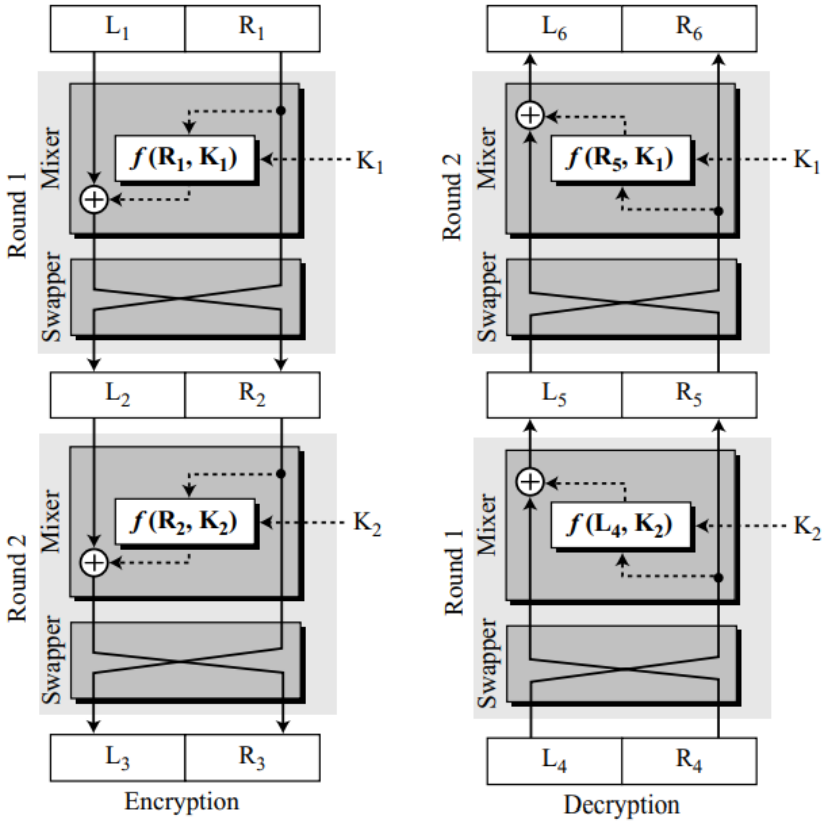
CRYPTOGRAPHY AND NETWORK SECURITY
VI SEM -20CS6PCCNS
SCHEME & SOLUTIONS

1. Demonstrate the encryption and decryption process in Feistel cipher with a neat figure.

   Solution:



The given plaintext is divided into blocks. Each block in turn is divided into two halves- left and right. A mixer xors the left half with the result of f(R1,K1) which is a function involving the right half of the data and the key1. The next operation done is swapping on the resulting data. These swapped halves act as input to the Round2. Note that there are two round keys, K1 and K2. The keys are used in reverse order in the encryption and decryption.

Because the two mixers are inverses of each other, and the swappers are inverses of each other, it should be clear that the encryption and decryption ciphers are inverses of each other. However, let us see if we can prove this fact using the relationship between the left and right sections in each cipher. In other words, let us see if L6 = L1. and R6

= R1, assuming that L4 = L3 and R4 = R3 (no change in the ciphertext during transmission).

Figure – 3 Marks **Explanation – 2 Marks** **Total- 8 Marks**

2.a. Consider the plaintext "an exercise". Encrypt using the affine cipher. Use keys multiplicative key=15 and additive key =20 5 Marks

Solution:

$C = (P \times k1 + k2) \bmod 26$ $P = ((C - k2) \times k1^{-1}) \bmod 26$

K1=15, $15^{-1} \bmod 26$ using extended Euclidean = 7 mod 26

Encryption:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption	Decryption
a->0 x 15 + 20 mod 26 =20 --→U	U-> (20-20) mod 26 , 0 X 7 mod 26 =0 ->a
n->13 x 15 + 20 mod 26 =7 → H	H-> (7-20) mod 26, 13 X 7 mod 26 =13 ->n
e->4 x 15 + 20 mod 26 =2 →C	C -> (2-20) 8 X 7 mod 26 = 4 ->e
x->23 x 15 + 20 mod 26 =1 →B	B-> (1-20) mod 26, 7 X 7 mod 26= 23 → x
e->4 x 15 + 20 mod 26 =2 → C	C-> (2-20)mod 26, 8 X 7 mod 26 = 4 →e
r->17 x 15 + 20 mod 26 = 15 →P	P-> (15-20)mod 26, 21 X 7 mod 26 = 17 ->r
c->2 x 15 + 20 mod 26 = 24 →Y	Y-> (24-20)mod 26, 4 X 7 mod 26=2 ->c
i->8 x 15 + 20 mod 26 = 10 →K	K-> (10-20) mod 26, 16 X 7 mod 26 =8 ->i
s->18 x 15 + 20 mod 26 = 4 ->E	E-> (4-20) mod 26, 10 X 7 mod 26 =18 ->s
e->4 x 15 + 20 mod 26 =2 →C	C-> (2-20) mod 26, 8 X 7 mod 26=4 ->e

2.b. A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks. Explain.

Solution:

In Block ciphers, generally the message to be encrypted is first converted into bits. Depending on the block size say n adapted by the cipher the message is divided into blocks each of size n. When the number of bits are not exact multiples of the block size, additional junk bits are padded towards the end, to make the number of bits a perfect multiple of the block size.

Explanation : 2 Marks

Using eight bits for each character, |M|=8 x 2000 = 16000 bits. We have

|M| +|Pad| =0 mod 64 -> |Pad| = -16000 mod 64 =0. This means no padding is needed. The message is divided into 250 blocks **3 Marks**

Total- 5 Marks

2.c.

a. The size of the key domain is 26 + 10 = 36. The modulus is also 36. Alice needs to use the set Z_{36}.

b. The size of the key domain is 12; the domain is (1, 5, 7, 11, 13, 17, 19, 23, 25, and 29). The modulus is 36. Alice needs to use the set $Z_{36}*$.

c. The key domain is 36 × 12 = 432. The modulus is still 36. However, Alice needs to use Z_{36} for addition and Z_{36}* for multiplication.

PART C

3.a. Multiply the following n-bit words using polynomials. (11100) × (10000) using the efficient algorithm in GF(2^5). Use ($x^5 + x^2 + 1$) as modulus.

Solution:

Polynomial Method:

P2=11100 –> $x^4 + x^3 + x^2$ p1= 10000 -> x^4

Powers	**Operation**	**New Result**	**Reduction**
x^0 x P2		$x^4 + x^3 + x^2$	No
x^1 x P2	x X ($x^4 + x^3 + x^2$)	$x^5+x^4+x^3 + x^5 + x^2 + 1$ = $x^4+x^3+x^2+1$	Yes
x^2 x P2	x X ($x^4+x^3+x^2+1$)	$x^5+x^4+x^3+x+$ x^5+x^2+1 = $x^4+x^3+x^2+x+1$	Yes
x^3 x P2	x X ($x^4+x^3+x^2+x+1$)	$x^5+x^4+x^3+x^2+$ $x+x^5+x^2+1$ = x^4+x^3+x+1	Yes
x^4 x P2	x X (x^4+x^3+x+1)	$x^5+x^4 +x^2+$ $x+x^5+x^2+1$ **= x^4+x+1**	

P1 X P2 → **x^4+x+1**

Multiplication using n-bit words:

Powers	**Shift-Left Operation**	**Exclusive-Or**
x^0 x P2		11100
x^1 x P2	11000	11000 + 00101 =11101
x^2 x P2	11010	11010 + 00101

		=11111
x^3 x P2	11110	11110 + 00101 =11011
x^4 x P2	10110	10110 + 00101 **=10011**

P1 X P2 = 10011 -> **x^4+x+1**

3.b.

i)

PT= cr yp ta na ly si si st ob re ak ci ph er sx

CT=SD OZ BU CL VO HT HT TU DM DQ VA HB FN QD NS

CT = SDOZBUCLVOHTHTTUDMDQVAHBFNQDNS

ii) The ciphertext GEZXDS was encrypted by a Hill cipher with a 2 × 2 matrix. The plaintext is 'solved'. Find the key matrix.

First, $solved \rightarrow GEZXDS$ leads us to $18, 14, 11, 21, 4, 3 \rightarrow 6, 4, 25, 23, 3, 18$. Then, we have

$$\begin{bmatrix} 18 & 14 \end{bmatrix} K = \begin{bmatrix} 6 & 4 \end{bmatrix}$$
$$\begin{bmatrix} 11 & 21 \end{bmatrix} K = \begin{bmatrix} 25 & 23 \end{bmatrix}$$
$$\begin{bmatrix} 4 & 3 \end{bmatrix} K = \begin{bmatrix} 3 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix} K = \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix}$$

This gives

$$\begin{bmatrix} 11 & 21 \\ 4 & 3 \end{bmatrix}^{-1} = \frac{1}{-51} \begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} \equiv \begin{bmatrix} 3 & -21 \\ -4 & 11 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix} \pmod{26}$$

So,

$$K = \begin{bmatrix} 3 & 5 \\ 22 & 11 \end{bmatrix} \begin{bmatrix} 25 & 23 \\ 3 & 18 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 90 & 159 \\ 583 & 704 \end{bmatrix} \pmod{26}$$

Finally, we have

$$K = \begin{bmatrix} 12 & 3 \\ 11 & 2 \end{bmatrix}$$

If "**solv"** is considered / if complete plaintext is considered, key will be different.

4.a.

i) We know that "ab" → "GL". This means that 00 → 06 and 01 → 11

We can construct two equations from these two pieces of information:

$00 \times k_1 + k_2 \equiv 06 \pmod{26}$ $01 \times k_1 + k_2 \equiv 11 \pmod{26}$

Solving these two equations give us $k_1 = 5$ and $k_2 = 6$.

This means, $P = ((C - k_2) \times k_1^{-1}) \bmod 26 = ((C + 20) \times 21) \bmod 26$

Inverse of 5 in mod 26 is 21 (Extended euclidean)

Ciphertext: XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

Plaintext: the best of a fight is making up afterwards

ii) Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.

Solution:

q	r_1	r_2	r	t_1	t_2	t
$x+1$	x^5+x^2+1	x^4+x^3+1	x^3+x^2+x	0	1	$x+1$
x	x^4+x^3+1	x^3+x^2+x	x^2+1	1	$x+1$	x^2+x+1
$x+1$	x^3+x^2+x	x^2+1	1	$x+1$	x^2+x+1	x^3+x
x^2+1	x^2+1	1	0	x^2+x+1	x^3+x	1
	1	0		x^3+x	1	

The inverse is x^3+x.

4.a.
i) Prove that the group $G = \langle Z_{10}^*, X \rangle$ is a cyclic group with two generators, g = 3 and g = 7.

Solution:

Three cyclic subgroups can be made from the group $\mathbf{G} = \langle \mathbf{Z}_{10}^*, \times \rangle$. **G** has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $\mathbf{H_1} = \langle \{1\}, \times \rangle$, $\mathbf{H_2} = \langle \{1, 9\}, \times \rangle$, and $\mathbf{H_3} = \mathbf{G}$. The following show how we find the elements of these subgroups.

a. The cyclic subgroup generated from 1 is $\mathbf{H}_1$. The subgroup has only one element, the identity element.

$1^0 \bmod 10 = 1$ (stop: the process will be repeated)

b. The cyclic subgroup generated from 3 is $\mathbf{H}_3$, which is **G** itself.

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$ (stop: the process will be repeated)

c. The cyclic subgroup generated from 7 is $\mathbf{H}_3$, which is **G** itself.

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$ (stop: the process will be repeated)

d. The cyclic subgroup generated from 9 is $\mathbf{H}_2$. The subgroup has only two elements.

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$ (stop: the process will be repeated)

Hence the group G =<Z_{10} *, X> is a cyclic group with two generators, g = 3 and g = 7.

ii) Consider the plaintext = "Cryptography and Network Security" (ignore spaces) and the encryption key (3, 2, 6, 1, 5, 4). Find the decryption key and the cipher text.

Solution:

Given Encryption key is 3 2 6 1 5 4 , 0 0 0 1 0 0

1 2 3 4 5 6

Swap: 1 2 3 4 5 6

3 2 6 1 5 4

Reorder: **4 2 1 6 5 3** →**Decryption Key**

1 2 3 4 5 6

Crypto 2 17 24 15 19 14

Graphy 6 17 0 15 7 24

andnet 0 13 3 13 4 19

workse 22 14 17 10 18 4

curity 2 20 17 8 19 24

Ciphertext 24 17 14 2 19 15

0 17 24 6 7 15

3 13 19 0 4 13

17 14 4 22 18 10

17 20 24 2 19 8

yroctp

aryghp

dntaen

roewsk

ruycti YADRRRRNOUOYTEYCGAWCTHESTPPNKI