Assignment #1

Name :- Priyansh Vaishnav
Student ID :- 202151120

Prob. (1)

Given plaintext :- CRYPTOGRAPHY
And given permutation (π) is the secret key.

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$$

a) For Ciphertext :-
1st Character will be transpose to 3rd Character
&
Ciphertext :-
plaintext :- C R Y P T O G R A P H Y
Ciphertext :- Y T O A H C R R P P Y G

b) We know permutation is bijection & so inverse of π exists.

$$\pi^{-1} :- \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 8 & 1 & 10 & 2 & 3 & 12 & 7 & 4 & 9 & 5 & 11 \end{pmatrix}$$

Ciphertext :- Y T O A H C R R P P Y G
plaintext :- C R Y P T O G R A P H Y

2021511120
Priyansh Vaishnav

Date
Page

Prob. (2)

Given plaintext :-
WEAREINDIAN

Shift Cipher with key 4

$Enc(x,4) = (x+4) \% 26$

For W :- $(22+4) \% 26 = 0 = A$
For E :- $(4+4) \% 26 = 8 = I$
For A :- $(0+4) \% 26 = 4 = E$
For R :- $(17+4) \% 26 = 21 = V$
For I :- $(8+4) \% 26 = 12 = M$
For N :- $(13+4) \% 26 = 17 = R$
For D :- $(3+4) \% 26 = 7 = H$

Ciphertext :- AIEVIMRHMER

$Dec(C,4) = (C+26-4) \% 26$

For A = $(0+26-4) \% 26 = 22 = W$
For I = $(8+26-4) \% 26 = 4 = E$
For E = $(4+26-4) \% 26 = 0 = A$
For V = $(21+26-4) \% 26 = 17 = R$
For M = $(12+26-4) \% 26 = 8 = I$
For R = $(17+26-4) \% 26 = 13 = N$
For H = $(7+26-4) \% 26 = 3 = D$

Ciphertext :- AIEVIMRHMER
↳ After decryption :- WEAREINDIAN

Hence Verified!

Prob. (3)

Given plaintext :- WEAREINDIAN
Secret key :- CRICKET
We have to encrypt this using playfair Cipher

C	R	I	K	E
T	A	B	D	F
G	H	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

divided plaintext into pairs and adding 'x' string :-

WE AR EI ND IA NX

Now we ~~substitute~~ Transpose the string using playfair rules

Plaintext : WE AR EI ND IA NX
Ciphertext : ZR HA CK MF RB LZ

Ciphertext :- ZRHACKMFRBLZ

Decrypted text :- WE AR EI ND IA NX

plaintext string = decrypted text
Hence Encryption is validate.

20215120
Priyansh Vaishnav

Date
Page

Prob. (4)

$K = (a, b)$, where $0 \le a, b \le 25$

encryption $y = Enc_K(x) = (ax + b) \bmod 26$

decryption $x = Dec_K(y) = (y - b)a^{-1} \bmod 26$

→ a^{-1} is multiplicative inverse under modulo 26 if $gcd(a, 26) = 1$ then only a^{-1} exists. We want that cases for which decryption is not possible.

therefore $gcd(a, 26) \neq 1$

then

$a \in (0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24)$

and for all b such that $b \in [0, 26]$ decryption is not possible.

Decryption Algorithm for successful decryption →

$$x = Dec_K(y) = (y - b)a^{-1} \bmod 26$$

$$a * a^{-1} = 1 \bmod 26$$

We have to find different no. of keys.
We Assume that $K_1(a, b)$ & $K_2(l, m)$ having diff. keys.

$$ax + b = y \bmod 26 \quad \text{— (I)}$$

$$lx + m = y \bmod 26 \quad \text{— (II)}$$

$$(a - l)x + (b - m) = 0 \bmod 26$$

putting $x = 0$

$$(b-m) = 0 \bmod 26 \quad \text{—— (III)}$$

Maximum value of $(b-m)$ is 25

means Eq (III) satisfy only if $(b = m)$

$$(a-l)x = 0 \bmod 26$$
$$(a-l) = 0 \cdot x^{-1} \bmod 26$$
$$(a-l) = 0 \bmod 26$$

$l \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

maximum value of $(a-l) = 24$

means

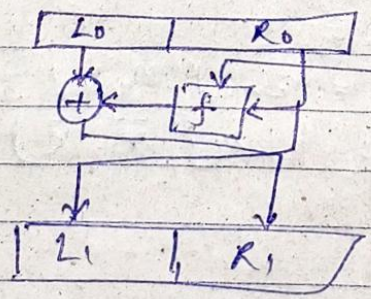
keys for $K_1(a, b)$ and $K_2(l, m)$ not be different.

So No. of different keys for which we will have the same plaintext-Ciphertext pair (x, y).

Prob (5)

$$C_1 = Enc(m, K)$$
$$C_2 = Enc(\bar{m}, \bar{K})$$

One Round of feistel Network of DES



$L_1 = R_0$

$R_1 = f(R_0, K_1) \oplus L_0$

20215120
Priyansh Vaishnav

Date
Page

if (m, k) and $(\bar{m}, \bar{k})$ are input to DES.
After 1st round

$$m = L_{0m} \| R_{0m} \quad , \quad \bar{m} = L_{0\bar{m}} \| R_{0\bar{m}}$$
$$L_{1m} = R_{0m} \quad , \quad L_{1\bar{m}} = R_{0\bar{m}}$$

$R_{0\bar{m}}$ and R_{0m} are complementary
Therefor L_{1m} & $L_{1\bar{m}}$ are also complementary

$$E(R_{0\bar{m}}) = \overline{E(R_{0m})}$$

$$f(\bar{m}, \bar{k}) = P(S(E(R_{0\bar{m}}) \oplus \bar{K}_1))$$
$$= P(S(\overline{E(R_{0m})} \oplus \bar{K}_1))$$
$$= P(S(E(R_{0m}) \oplus K_1))$$
$$f(\bar{m}, \bar{k}) = f(m, k)$$

$$R_{1m} = f(R_{0m}, K) \oplus L_{0m} \quad \text{— (i)}$$

$$R_{1\bar{m}} = f(R_{0\bar{m}}, \bar{K}) \oplus L_{0\bar{m}}$$
$$R_{1\bar{m}} = f(R_{0m}, K) \oplus L_{0\bar{m}}$$

$$R_{1\bar{m}} = \overline{R_{1m}}$$

Hence

$$C_1 = Enc(m, k)$$
$$C_2 = Enc(\bar{m}, \bar{k})$$

$$C_2 = \overline{C_1}$$

Prob. (6)

Ciphertext :- ~~A F I N E~~
A F I T I F W F

decrypt this using brute force

$$P = (C + 26 - K) \bmod 26$$

K = 1

For A :- $(0 + 26 - 1) \bmod 26 = 25 = Z$
For F :- $(5 + 26 - 1) \bmod 26 = 4 = E$
For I :- $(8 + 26 - 1) \bmod 26 = 7 = H$
For T :- $(19 + 26 - 1) \bmod 26 = 18 = S$
For W :- $(22 + 26 - 1) \bmod 26 = 22 = V$
P = ZEHSHEVE (meaningless)

K = 2

For A :- $(0 + 26 - 2) \bmod 26 = 24 = Y$
For F :- $(5 + 26 - 2) \bmod 26 = 3 = D$
For I :- $(8 + 26 - 2) \bmod 26 = 6 = G$
For T :- $(19 + 26 - 2) \bmod 26 = 18 = S$
For W :- $(22 + 26 - 2) \bmod 26 = 20 = U$
P = YDGRGDUD (meaningless)

K = 3

For A :- $(0 + 26 - 3) \bmod 26 = 23 = X$
For F :- $(5 + 26 - 3) \bmod 26 = 2 = C$
For I :- $(8 + 26 - 3) \bmod 26 = 5 = F$
For T :- $(19 + 26 - 3) \bmod 26 = 12 = Q$
For W :- $(22 + 26 - 3) \bmod 26 = 19 = T$
P = XCFQFCTC (meaningless)

K = 4

For A :- $(0 + 26 - 4) \bmod 26 = 22 = W$

For F : (5+26-4) mod 26 = 1 = B
For I : (8+26-4) % 26 = 4 = E
For T : (19+26-4) % 26 = 15 = P
For W : (22+26-4) % 26 = 18 = S
P = WBEPEBSB (meaningless)

K=5
For A : (0+26-5) % 26 = 21 = V
For F : (5+26-5) % 26 = 0 = A
For I : (8+26-5) % 26 = 3 = D
For T : (19+26-5) % 26 = 14 = O
For W : (22+26-5) % 26 = 17 = R
P = VADDOARA (meaningful)
K=5 Answer

Prob. (7) Given plaintext = HILL
Ciphertext = XIYJ

$$C = K.P \bmod 26$$
$$K = C P^{-1} \bmod 26$$
$$K = \begin{bmatrix} X & Y \\ I & J \end{bmatrix} \begin{bmatrix} H & L \\ I & L \end{bmatrix}^{-1} \bmod 26$$
$$K = \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 7 & 11 \\ 8 & 11 \end{bmatrix}^{-1} \bmod 26$$

$$K = \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 8/11 & -7/11 \end{bmatrix} \bmod 26$$

$$K = (-11)^{-1} \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} \bmod 26$$

$$K = (+15)^{-1} \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} \bmod 26$$

multiplicative inverse of 15 mod 26

$$\begin{array}{r|l} 15 & 26 \\ & 15 \\ \hline & 11 \end{array}\quad 1$$

$$\begin{array}{r|l} 11 & 15 \\ & 11 \\ \hline & 4 \end{array}\quad 1$$

$$\begin{array}{r|l} 4 & 11 \\ & 8 \\ \hline & 3 \end{array}\quad 2$$

$$\begin{array}{r|l} 3 & 4 \\ & 3 \\ \hline & 1 \end{array}\quad 1$$

$1 = 4 - 1.3$
$1 = 4 - (11 - 4\times2)$
$1 = 4 - 11 + 4\times2$
$1 = 4\times3 - 11$
$1 = 3\times(15 - 11\times1) - 11$
$1 = 3\times15 - 4\times11$
$1 = 3\times15 - 4(26 - 15\times1)$
$1 = 3\times15 - 4\times26 + 4\times15$
$1 = 7\times15 - 4\times26$

multiplicative inverse of 15 mod 26 = 7

$$K = 7 \begin{bmatrix} 61 & -85 \\ 16 & -25 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 & 3 \\ 8 & 7 \end{bmatrix}$$

Ans

Prob. (8)

a) gcd (222, 18)

$$18 \overline{)222} \; (12 \qquad 6 \overline{)18} \; (3$$
$$\underline{18} \qquad\qquad \underline{18}$$
$$42 \qquad\qquad 0$$
$$\underline{36}$$
$$6$$

remainder = 0

gcd (222, 18) = 6

(b) $1 = 33x_0 + 13y_0$

$$13 \overline{)33} \; (2 \qquad 7 \overline{)13} \; (1 \qquad 6 \overline{)7} \; (1$$
$$\underline{26} \qquad\quad \underline{7} \qquad\quad \underline{6}$$
$$7 \qquad\quad 6 \qquad\quad 1$$

gcd (33, 13) = 1

$1 = 7 - 6.1$
$1 = 7 - (13 - 7.1)$
$1 = 2.7 - 13$
$1 = 2(33 - 13.2) - 13$
$1 = 2.33 - 5.13$

$x_0 = 2, \; y_0 = -5$

(c) multiplicative inverse of 5 under modulo 26

$$5\overline{)26}\,(5$$
$$\underline{25}$$
$$1$$

$$\gcd(5, 26) = 1$$

$$1 = 5.x + 26.y$$
$$1 = 1.26 - 5.5$$
$$1 = -5.5 + 1.26$$

multiplicative inverse of 5 under modulo 26
PS -5
or
we can say multiplicative inverse of 5 under modulo 26 is $-5+26 = \underline{21}$

Prob. (2) Applying AES Subbyte on D3

we have $Q(x) = x^8 + x^4 + x^3 + x + 1$

$(D3)_{16} = (11010011)_2$

$P(x) = x^7 + x^6 + x^4 + x + 1$

$$x^7+x^6+x^4+x+1 \;\overline{)}\; x^8 + x^4 + x^3 + x + 1 \;(\; x+1$$
$$x^8 + x^7 + x^5 + x^2 + x$$
$$x^7 + x^5 + x^4 + x^3 + x^2 + 1$$
$$x^7 + x^6 + x^4 + x + 1$$
$$x^6 + x^5 + x^3 + x^2 + x \quad \text{Ans}$$

$$x^6+x^5+x^3+x^2+x \;\overline{)}\; x^7 + x^6 + x^4 + x + 1 \;(\; x$$
$$x^7 + x^6 + x^4 + x^3 + x^2$$
$$x^3 + x^2 + x + 1$$

$$x^3+x^2+x+1 \;\overline{)}\; x^6 + x^5 + x^3 + x^2 + x \;(\; x^3 + x$$
$$x^6 + x^5 + x^4 + x^3$$
$$x^4 + x^2 + x$$
$$x^4 + x^3 + x^2 + x$$
$$x^3$$

20215120
Priyansh Vaishnav

Date
Page

$$x^3+x+1$$
$$x^3+x^2+x+1 \;\overline{)}\; x^6+x^5+x^3+x^2+x$$
$$x^6+x^5+x^4+x^3$$
$$x^4+x^2+x$$
$$x^4+x^3+x^2+x$$
$$x^3$$
$$x^3+x^2+x+1$$
$$x^2+x+1$$

$$x^2+x+1 \;\overline{)}\; x^3+x^2+x+1 \;(\; x$$
$$x^3+x^2+x$$
$$1$$

$$1 = (x^3+x^2+x+1) + x(x^2+x+1)$$
$$1 = (x^3+x^2+x+1) + x\left((x^6+x^5+x^3+x^2+x) + (x^3+x^2+x+1)(x^3+x+1)\right)$$
$$1 = (x^3+x^2+x+1)(x^4+x^2+x+1) + x(x^6+x^5+x^3+x^2+x)$$
$$1 = \{P(x) + x(x^6+x^5+x^3+x^2+x)\}(x^4+x^3+x+1) + x(x^6+x^5+x^3+x^2+x)$$
$$1 = (x^4+x^2+x+1)\cdot P(x) + (x^6+x^5+x^3+x^2+x)(x^5+x^3+x^2)$$
$$1 = (x^4+x^2+x+1)P(x) + \{G(x) + (x+1)P(x)\}(x^5+x^3+x^2)$$
$$1 = (x^5+x^3+x^2)G(x) + P(x)\left[x^4+x^2+x+1 + (x+1)(x^5+x^3+x^2)\right]$$
$$1 = (x^5+x^3+x^2)G(x) + P(x)(x^6+x^5+x+1)$$

inv of $P(x) = x^6+x^5+x+1 = 01100011$

2021511120
Priyansh Vaishnav

$c = (01100011)_2$

for $i = 0$ to 7

$m_i = (b_i + b_{(i+4)\%8} + b_{(i+5)\%8} + b_{(i+6)\%8} + b_{(i+7)\%8} + c_i) \bmod 2$

$b_i = c_i$

$m_0 = (1+0+1+1+0+1) \bmod 2 = 0$

$m_1 = (5) \bmod 2 = 1$

$m_2 = (3) \bmod 2 = 1$

$m_3 = (2) \bmod 2 = 0$

$m_4 = 2 \bmod 2 = 0$

$m_5 = 3 \bmod 2 = 1$

$m_6 = 3 \bmod 2 = 1$

$m_7 = 2 \bmod 2 = 0$

Subbyte (D3) $= m_7 m_6 m_5 m_4 m_3 m_2 m_1 m_0$

$= (01100110)_2$

$= (66)_{16}$

Hence proved.

Prob. (10) AES-mixcolumn (33, 42, 66, 24) $= (P_0\ P_1\ P_2\ P_3)$

$33 = 00100001 = x^5 + 1$

$42 = 00101010 = x^5 + x^3 + x$

$66 = 01000010 = x^6 + x$

$24 = 00011000 = x^4 + x^3$

$P_0 = \left(2(x^5+1) + (x+1)(x^5+x^3+x) + (x^6+x) + (x^4+x^3)\right) \bmod (x^8+x^4+x^3+x+1)$

$P_0 = (x^6+x^5+x^2+x) \bmod (x^8+x^4+x^3+x+1)$

$P_0 = x^6+x^5+x^2+x = 01100110 = 102$

$P_1 = \left((x^5+1) + 2(x^5+x^3+x) + (x+1)(x^6+x) + x^4+x^3\right) \bmod (x^8+x^4+x^3+x+1)$

20215120
Priyansh Vaishnav

Date
Page

$P_1 = (x^7 + x^5 + x^3 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$

$P_1 = x^7 + x^5 + x^3 + x + 1 = 10101011 = 171$

$P_2 = \{(x^5 + 1) + (x^5 + x^3 + x) + x(x^6 + x) + (x+1)(x^4 + x^3)\}$
$\bmod (x^8 + x^4 + x^3 + x + 1)$

$P_2 = (x^7 + x^5 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$

$P_2 = x^7 + x^5 + x^2 + x + 1 = 10100111 = 167$

$P_3 = \{(x+1)(x^5+1) + (x^5 + x^3 + x) + (x^5 + x) + x(x^4 + x^3)\}$
$\bmod (x^8 + x^4 + x^3 + x + 1)$

$P_3 = x^5 + x^4 + x^3 + x + 1 = 00111011 = 59$

AES-mix column $(33, 42, 66, 24) = (162, 171, 167, 59)$

Prob. (11) $f(a,b) : \mathbb{Z}_p \to \mathbb{Z}_p \quad a, b \in \mathbb{Z}_p$

$f_{(a,b)}(x) = (ax + b) \bmod p = y$

$f_{(a,b)}(x') = y' \quad$ and $x \neq x'$

$$ax + b = y \bmod p$$
$$ax' + b = y' \bmod p$$

$$a(x' - x) = (y' - y) \bmod p$$

$\because x' \neq x$

inverse of $(x'-x)$ under modulo p exist iff $gcd(x'-x, p) = 1$

∵ p is a prime no.

Therefore $gcd(x'-x, p) = 1$

and inverse of $(x'-x)$ exist

$$a = (y'-y)(x'-x)^{-1} \bmod p$$

b can be derive either from the eqn

$ax+b = y \bmod p$ or $ax'+b = y' \bmod p$

Prob (12) $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$

$h(x) = xA$

$$[x_1\ x_2\ \dots\ x_7] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [0\ 1\ 0\ 1] \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} x_1 + x_2 + x_3 + x_4 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix} \bmod 2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Because all are under modulo 2 operation so
We conclude that
(x_1, x_2, x_3, x_4) ~~either~~ add 0
i) all zero ii) any two are 1 iii) all 4 are 1

Same as for
(x_3, x_4, x_5, x_6)
In (x_2, x_3, x_4, x_5) either any one is 1 or any three is 1
~~possible cases~~ Same as for (x_4, x_5, x_6, x_7)
Possible cases

x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	1	1	1	0	0	0
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	0	0	0	0	1
0	0	1	1	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	1	1
0	0	0	0	1	1	1

These 8 Tuples are pre-image of [0 1 0 1] under $h(x) = xA$

20215120
Priyansh Vaishnav

Prob. (13) $h_1 : \{0,1\}^{2m} \longrightarrow \{0,1\}^{m}$

We are assuming a contradiction that

$h_2 : \{0,1\}^{4m} \rightarrow \{0,1\}^{m}$ is not a collision resistant $\quad x_1 \neq x_2$ & $h_2(x_1) = h_2(x_2)$

We define x_1 & x_2 as

$$x_1 = x_{11} \,||\, x_{12}$$
$$x_2 = x_{21} \,||\, x_{22}$$

$x_{11}, x_{12}, x_{21}, x_{22} \in \{0,1\}^{2m}$

$\because \quad h_2(x_1) = h_2(x_2)$

$$h_1[h_1(x_{11}) || h_1(x_{12})] = h_1[h_1(x_{21}) || h_1[x_{22}]]$$

Given that $h_1(x)$ is collision resistant i.e it is hard to compute $x_a \neq x_b$ s.t. $h_1(x_a) = h_1(x_b)$

$$h_1(x_{11}) || h_1(x_{12}) = h_1(x_{21}) || h_1(x_{22})$$
$$h_1(x_{11}) = h_1(x_{21})$$
$$h_1(x_{12}) = h_1(x_{22})$$

$\because h_1(x)$ is collision resistant

$$x_{11} = x_{21}$$
$$x_{12} = x_{22}$$

Contradiction

$h_2(x)$ is collision resistant fxn.