2021S1192
Archit Verma

DOMS | Page No.
Date / /

Ques 1 Plaintext :- CRYPTOGRAPHY

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

(a) Here our key is a transposition matrix. The key says 1st character will be replaced by 3rd & so on.

(Cipher text :-) = YTOAHCRRPPYG

(b) Here decryption is possible. Since the permutation here is a bijection & its inverse exist, we can use π^{-1} as key for decryption. It will be nothing just vertical flip of the keys.

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

we will again apply same technique just using π^{-1} as key on cipher text & we will get our decrypted text.

Ques 2 Question :- 2

In shift cipher encoding & decoding for key k is done as

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

$dec(x,k) = (x+26-k) \% 26$

where x corresponds to integer corresponding to alphabets.

Plaintext :- WEAREINDIAN

key :- 4

D021511192
Archit verma

Enc (W,4) = (22+4)·mod 26 = 0 = A
Enc (E,4) = (4+4)·mod 26 = 8 = I
Enc (A,4) = (0+4)·mod 26 = 4 = E
Enc (R,4) = (17,4)·mod 26 = 21 = V
Enc (I,4) = 12 = M
Enc (N,4) = 7 = R
Enc (D,4) = 7 = H

Encryption of WEAREINDIAN TB:-

AIEVIMRHMER

Similarly decrypting:-

(Dec (A,4) = (0+26-4) = mod 26 = 22 = W
Dec (I,4) = 4 = E
Dec (E,4) = 0 = A
Dec (V,4) = (21,4) = 17 = R
Dec (M,4) = 8 = I
Dec (R,4) = 13 = N
Dec (H,4) = 3 = D

So decryption of AIEVIMRHMER is WEAREINDIAN

20215192
Archit Varma

Problem:- 3

Playfair cipher:-
Plaintext :- WEAREINDIANS
Secret key :- CRICKET

Playfair matrix:-(5x5) :-

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

Playfair string :- WE AR EI ND IA NX

Rules:-

If both lie in same row take the right one of them. If a word letter lies at last take the first one.

If both lie in same column take the one at below them. If a letter lies at bottom take the top one.

If o.w., make a rectangle covering both and take the letter at opposite corner in same same row.

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

WF

W → Z F → C I → R
F → R I → K A → B.
A → H N → M N → L
R → A D → F X → Z

9021 CT192

Archit Varma

So our ciphertext :- 2RHACKMFRBL2

Now decrypting.. (notice for same row & column now the direction reverses & for rectangle rule remains same)

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

2R HA CK MF RB L2

2 → W

R → E

H → A

A → R

C → E

K → I

M → N

F → D

R → I

B → A

L → N.

2 → X.

So we get the same decrypted text "WEAREINDIANX"

2021511192
Archit Verma

DOMS | Page No.
Date : / : /

Problem:-4

We know that for key(a,b)
$y = enc(x) = (ax+b) \bmod 26$ and a & 26 are coprime.
a^{-1} will be required for decryption such that
$x = dec(y) = ((y-b)a^{-1}) \bmod 26$
But finding inverse will not be possible unless a & 26 are coprime.
So decryption is not possible for cases where
$gcd(a,26) \neq 1$

Decryption algorithm when we can have successful decryption is

$x = Dec_k(y) = [a^{-1}(y-b)] \bmod 26$
where
$a * a^{-1} = 1 \bmod 26$

Now we need to find different keys for which we have some Plaintext-ciphertext pair (x,y)

for keys $k_1(a,b)$ & $k_2(a',b')$ assume $k_1 \neq k_2$

So
$ax+b = y \bmod 26$ — (1)
$a'x+b' = y \bmod 26$ — (2)
sub (1) from (2)
$(a'-a)x + (b'-b) = 0 \bmod 26$ — (3)

Now $x \in \{0,1,\ldots 25\}$. let $x=1$ but $x=0$ in (3)
$(b'-b) = 0 \bmod 26$ — (4)
as $b', b \in \{0,1,2,\ldots 25\}$
so maximum value of b or b' can be 25

7.21 3/1/22

Archi Verma

So (IV) holds when $b' = b$

Now as $x \in \{0, 1, \ldots 25\}$ and eqn (3) is

Note:- eqn should satisfy for all $i \in x$.

$(a'-a)x + (b'-b) \equiv 0 \bmod 26$

So now put $(b'=b)$ in (3) we get

$(a'-a)x \equiv 0 \bmod 26$

$a'-a) \equiv 0 \cdot x^{-1} \bmod 26$

$(a'-a) = 0 \bmod 26$ (x^{-1} is integer)

so $a'=a$

~~so for a given~~

so we found $a' = a$ & $b' = b$ so $k_1 = k_2$ which contradict our assumption.

Hence there is no such pair such that keys are different but corresponding cipher & plaintext pair are same.

2021311932
Archit Verma

DOMS | Page No.
Date / /

Question: 5

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

The key scheduling algorithm of DES removes parity bit out of 64-bit key. It then permute then left circular shift subsitute to finally generate round keys.

Permutation & subsitution will not affect the individual bits

but for left circular shift.

$LCS(x_1 \cdots x_{32}, 2) = x_3 x_4 \cdots x_{32} x_1 x_2$.

& $LCS(\bar{x}_1 \cdots x_{32}, 2) = \bar{x}_3 \bar{x}_4 \cdots \bar{x}_{32} \bar{x}_1 \bar{x}_2$.

Now if we generate round keys from K & $\bar{K}$ the round keys generated will also be complementary.

Now consider a feistel network of DES.

$L_1 = R_0$
$R_1 = f(R_0, k_1) \oplus L_0$

Now consider (M, K) & $(\bar{M}, \bar{K})$ as input to des.

$M = L_0 \| R_0$
$\bar{M} = L_0 \bar{} \| R_0 \bar{}$

and

$L_1 = R_0$ & $L_1 \bar{} = R_0 \bar{}$

Here we can clearly see L_1 & $L_1 \bar{}$ are complementary.

2021571192
Archit Verma

Now let's look at our function Part. i.e.
$f(R_{0M}, K)$, $f(R_{0\bar{M}}, \bar{K})$

R_{0M} is mainly XOR of L_{0M} & K.
Suppose L_{0M} is $x_{32M} x_{33} - - - x_{63M}$.
on XOR $K_{32M} \cdot K_{33M} - - K_{63M}$.
So our digit becomes $Y_{32M}\ Y_{33M} - - - Y_{63M}$

Now for complement $R_{0\bar{M}}$ & $\bar{K}$
we had $x_{32\bar{M}} x_{33\bar{M}} - - x_{63\bar{M}}$
& $k_{32\bar{M}}\ k_{33\bar{M}} - - - K_{63\bar{M}}$

so bits in both R_{0M} & $\bar{K}$ are flipped and when we XOR it will lead to same result if the bits were not flipped.
so $f(\bar{M}, \bar{K}) = f(M, K)$ — (1)
$(A \oplus B = \bar{A} \oplus \bar{B},)$

$R_{1M} = f(R_{0M}, K_1) \oplus L_{0M}$ and $R_{1\bar{M}} = f(R_{0\bar{M}}, \bar{K}_1) \oplus L_{0\bar{M}}$

but from (1) $f(R_{0M}, K_1)$ & $f(R_{0\bar{M}}, \bar{K}_1)$ are equal

So here
$R_{1M} = \overline{R_{1M}}$ as we are XORing same value with L_{0M} & $L_{0\bar{M}}$ so results will be complements.

$\therefore L_{1M} \| R_{1M}$ will be complementary to $L_{1\bar{M}} \| R_{1\bar{M}}$.

So for
$C_1 = (M, K)$ & $C_2 = (\bar{M}, \bar{K})$

2021719

Archit Verma

we have

$C_1 = \overline{C_2}$

Question 6

a

AFITIFWF

Decrypt using K=1 :→ ZEHSEVE

Decrypt using K=2 :→ YDGRTDUD

Decrypt using K=3 :→ XCFQFCTC

Decrypt using K=4 :→ WBEPEBSB

Decrypt using K=5 :→ VADODARA

so our plaintext is VADODARA & Key = 5

Question :- 7

a

In hill cypher we use a matrix to encrypt our plain text as

$C = A \cdot P \bmod 26$

so $A = CP^{-1} \bmod 26$

→ Plaintext :- HILL

→ Corresponding ciphers :- XIYJ

$$A = \begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 7 & 11 \\ 5 & 11 \end{bmatrix}^{-1} \bmod 26.$$

Now finding :-

$$\begin{bmatrix} 7 & 11 \\ 5 & 11 \end{bmatrix}^{-1}$$

$\det = (77 - 55)$

$= (-11)$

converting it to +ve

$(-11+26) - 26 = 15$

2021511132
Archit Verma

Adj (A)

$$\begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix}$$

Inverse

$$(15)^{-1}\begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix}$$

but 15^{-1} is nothing but multiplicative inverse of 15.

$26 = 15\times1+11$	Now backwards
$15 = 11\times1+4$	$1 = 4-3$
$11 = 4\times2+3$	$1 = 4-(11-2\times4)$
$4 = 3\times1+1$	$1 = 3-4\times11$
$3 = 1\times3+0$	$1 = 3(15-11)-11$
~~flow back~~	$1 = 3\cdot15-4\cdot(26-15)$
	$1 = 7\cdot15-4\cdot26$

$15^{-1} = 7$.

Now

$$A = (15^{-1})\begin{bmatrix} 23 & 24 \\ 8 & 9 \end{bmatrix}\cdot\begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} \mod 26$$

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

2021511gL
Archit Verma

DOMS | Page No. | Date / /

(a) ~~gcd, a~~

Question 8

a

Gcd (222, 18)

$$
\begin{array}{r|l}
18 & 222 \;(12 \\
 & 18 \\
\hline
 & 42 \\
 & 36 \\
\hline
6 & 18 \;(3 \\
 & 18 \\
\hline
 & 0
\end{array}
$$

Gcd is 6

(b) x_0, y_0 s.t $1 = 33x_0 + 13y_0$

we can see that 13 & 33 are coprime so their gcd will be 1

So by bezout's identity

fo (x,y) if gcd (x,y) = d

their exist some a & b s.t

$d = ax + by$.

So here.

$33 = 13 \times 2 + 7$

$13 = 7 \times 1 + 6$

$7 = 6 \times 1 + 1$

$6 = 1 \times 6 + 0$.

Now backwards

$1 = 7 - 1.6$

$1 = 7 - (13 - 1.7)$

$1 = 2.7 - 1.13$

$1 = 2(33 - 2.13) - 1.13$

$1 = 2.33 - 5.13$

So our x_0 and y_0 are

$x_0 = 2$

$y_0 = -5$.

2021511192
Archit Verma

(c) Here again 5 & 26 are clearly coprime, so gcd b/w them will be 1

$26 = 5 \times 5 + 1$

$5 = 1 \times 5 + 0$.

$1 = 26 - 5 \times 5$

So for $1 = s.x + 26.y$

we had $x = -5$ & $y = 1$

so multiplicative inverse is -5 which is equivalent to $-5 + 26 = 21$

Question — 3

Here

$c = (D3)_{16}$

primitive polynomial : $x^8 + x^7 + x^3 + x + 1$

converting hexademical to binary to get polynomial

$(D3)_{16} = (1101\ 0011)_2$.

polynomial corresponding to it :—

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

Now find its the inverse.

2021511932
Archit Verma

DOMS Page No.
Date / . . /

$x^7+x^6+x^4+x+1 \;\big)\; x^8+x^4+x^3+x+1 \;\big(\; x+1$

$x^8+x^7+x^5+x^4+x$

$x^7+x^5+x^4+x^3+x^2+1$

$x^7+x^6+x^4+x+1$

$x^6+x^5+x^3+x^2+x \;\big)\; x^7+x^6+x^4+x+1 \;\big(\; x$

$x^7+x^6+x^4+x^3+x^2$

x^3+x^2+x+1

Now we will apply extended

$x^3+x^2+x+1 \;\big)\; x^6+x^5+x^3+x^2+x \;\big(\; x^3+x+1$

$x^6+x^5+x^4+x^3$

x^4+x^2+x

$x^4+x^3+x^2+x$

x^3

x^3+x^2+x+1

$x^2+x+1 \;\big)\; x^3+x^2+x+1 \;\big(\; x$

x^3+x^2+x

$1 \;\big)\; x \;\big(\; x$

x

0

Now with extended euclidean

2 r_1 r_2 r_0 t_1 t_2 t_0

$x^8+x^4+x^3+x+1$ x^3+x^2+1

$x^6+x^5+x^2$ / $+x^2+x+1$ | $(x^3+x+1)(x^2+x+1)+x+1$

$x^5+x^3+x^2+x^4+x^2+x+x^3+x+1$

$d_0 = t_1 \oplus 2t_2$

(20213192 Rachit Verma)

q_0	r_1	r_2	r_0	t_1	t_2	t_0
$x+1$	$x^6+x^4+x^3+x+1$	$x^5+x^4+x^2+1$	$x^6+x^5+x^3+x^2+x$	0	1	$x+1$
x	$x^5+x^4+x^3+1$	$x^6+x^5+x^3+x^2+x$	x^3+x^2+x+1	1	$x+1$	x^2+x+1
x^3+x+1	$x^6+x^5+x^3+x^2+x$	x^3+x^2+x+1	x^2+x+1	$x+1$	x^2+x+1	x^5+x^4+x
x	x^3+x^2+x+1	x^2+x+1	1	x^2+x+1	x^5+x^4+x	x^6+x^5+x+1
x	x^2+x+1	1	0	x^5+x^4+x	x^6+x^5+x+1	

So its inverse is x^6+x^5+x+1

The binary representation is

$(0110\ 0011)_2$

Now converting to Hexadecimal

$(0110\ 0110)_2 = (66)_{16}$

Problem - 10

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 33 \\ 42 \\ 66 \\ 24 \end{bmatrix}$$

Here we take $1 \to 1$, $2 \to x$, $3 \to (x+1)$

converting into binaries our plaintext

$33 = (00100001) \to x^5+1$

$42 = (00101010) \to x^5+x^3+x$

$(66) = (01000010) \to x^6+x$

$24 = (00011000) \to x^4+x^3$

2021115
Architecture

DOMS | Page No.
Date / /

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \begin{bmatrix} x^5+1 \\ x^5+x^3+x \\ x^6+x \\ x^4+x^3 \end{bmatrix}$$

$y_0 = (x^5+1)(x) + (x^5+x^3+x)(x+1) + (x^6+x)(x^4+x^3)$

$= x^6 + x + x^6 + x^4 + x^2 + x^5 + x^3 + x + x^6 + x^4 + x^4 + x^3$

$= (x^6 + x^5 + x^2 + x)$

there is 8 is not present so it will not require any replacement & $x^8 = x^4 + x^3 + x + 1$

$\boxed{(y_0) = x^6 + x^5 + x^2 + x}$

$y_1 = (x^5+1) + (x^5 + x^3 + x)(x) + (x^6 + x)(x+1) + (x^4 + x^3)$

$= x^5 + 1 + x^6 + x^3 + x^2 + x^7 + x^6 + x^6 + x + x^4 + x^3$

$= x^7 + x^5 + x^4$

$= \boxed{x^7 + x^5 + x^4 + x + 1}$

$y_2 = (x^5+1) + (x^5 + x^3 + x) + (x^7 + x^2) + (x^7 + x^4 + x^4 + x^3)$

$= x^7 + x^5 + x^2 + x + 1$

$y_3 = (x^6 + x + x^5 + 1) + (x^5 + x^3 + x) + (x^4 + x^3) + (x^5 + x^4)$

$\boxed{x^5 + x^4 + x^3 + x + 1}$

DOMS Page No.
Date / /

So in binary.

$y_0 = (01100110) = 102$
$y_1 = (10110011) = 179$
$y_2 = (10100111) = 167$
$y_3 = (00111011) = 59$

Problem - 11

$f(a,b) : Z_p \to Z_p$ by the rule $f(a,b)\,x = ax+b \bmod p$.

Now for (x, x')

$f(x) = y$
$f(x') = y'$.

$x \neq x'$

We need to prove if (a,b) can be found here

$(ax+b) \equiv y \bmod p$ — (I)
$(ax'+b) \equiv y' \bmod p$ — (II)

Sub (II) from (I)

$a(x'-x) \equiv (y'-y) \bmod p$.

as $x' \neq x$ so $x'-x \neq 0$

Her p is a prime number so
gcd (p, (x'-x)) is 1.
As gcd is 1 so we can find

2021111192
Archit Verma

the inverse. such that $(x'-x)^{-1}(x-x) \equiv 1$ (by bezout's identity).

so:

$$a(x'-x^*) \equiv (y'-y^*) \bmod p.$$

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

where $(y'-y)$, p are known & $(x'-x)$ can be calculated

$\therefore$ a can be found.

on getting a we can put it in (I) or (II) to get b.

so a,b can be found

$\therefore$ proved.

R2215192
Archit Verma

problem - 12

Here let $x \in (Z_2)^7$

let denote

$x = [x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7]$

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Now given

for $(Z_2)^7 \rightarrow (Z_2)^4$

$h(x) = xA$

$[x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7]$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

mod 2 = [0 1 0 1]

for ease & convinience let's work on transpose so we need to deal with one column only.

$$\begin{bmatrix} x_1 + x_2 + x_3 + x_4 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \begin{matrix} \text{---(1)} \\ \text{---(2)} \\ \text{---(3)} \\ \text{---(4)} \end{matrix}$$

2021511192

Archit Verma

DOMS | Page No. | Date 1 1

from (II) & (I)

$x_1 = x_5 + 1$

~~from (III) & (IV)~~

~~$x_1 + x_3 + x_5 + x_6 = 0$~~

~~$1 + x_3 + x_6 = 0$~~

~~or~~

from (III) & (II)

$x_2 = x_6 + 1$

~~from (IV) & (III)~~

~~$x_3 = x_2 + 1$~~

Now each table becomes

$$\begin{bmatrix} x_5 + x_6 + x_7 + x_4 + 1 \\ x_6 + x_7 + x_4 + x_5 \\ x_7 + x_4 + x_5 + x_6 + 1 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \rightarrow (6)$$

Now from (6) it is clear either one of x_4, x_5, x_6, x_7 are 1 or 3 of them are 1.

So all possible combination of x_4, x_5, x_6, x_7 are :-

$\{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,0), (1,1,0,1), (1,0,1,1), (0,1,1,1)\}$

Now using their relation with x_1, x_2, x_3 we have following 8 possibility.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	1	1	1	1	0	0	0
2	0	1	1	0	1	0	0
3	1	0	1	0	0	1	0
4	1	1	0	0	0	0	1
5	0	0	1	1	1	1	0
6	0	1	0	1	1	0	1
7	1	0	0	1	0	1	1
8	0	0	0	0	1	1	1

2021/1192
Architecture

Let's assume.

Question - 13

We will prove it by contradiction.

Here

$h_1 : \{0,1\}^{2m} \rightarrow \{0,1\}^n$ is collision resistant

$h_2 : \{0,1\}^{4n} \rightarrow \{0,1\}^m$:-

Our

$x \in \{0,1\}^{4n}$.

$x = x_1 \| x_2 \quad x_1, x_2 \in (0,1)^{2m}$.

To show h_2 is collision resistance.

let us assume two x values

x_{11}, x_{22} and $x_{11} \neq x_{22}$.

$x_{22} = x$ $\quad x_{11} = x_1 \| x_2$

$x_{22} = x_1' \| x_2'$

Let h_2 is suppose not be collision resistant:

$h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$

as $h_2(x)$ is not collision resistant we will have some x_{11} & x_{22} for which

$h_2(x_{11}) = h_2(x_{22})$

$h_2[h_1(x_1) \| h_1(x_2)] = h_2[h_1(x_1') \| h_1(x_2')]$ — (1)

2021571192
Aarchit Verma.

Since h_2 is collision resistance
$h_1(x_1') = h_1(x_1)$ & $h_1(x_2'') = h_1(x_2)$
only when $x_1' = x_1$ & $x_2' = x_2$
& $h(x_1') \| h_1(x_2') = h_1(x_1) \| h_2(x_2)$ only when they are equal.
So we have
$x_1' = x_1$
& $x_2' = x_2$
but this contradicts that fact that they are not equal. This contradiction arised due to fact that we took wrong assumption that h_2 is not collision resistant.
Hence h_2 is collision resistant.