CRNS Assignment (1)

19DCS008

Q-1 Calculate the Cipher text for following:-

(1) Plain Text = attack is today

Algorithm = Additive Cipher

Key = 13

=> Logic for Encryption: $E(P,K) = (P+K)\%026$

* For P.T. a => $E(a,13) = (0+13)\%026$
$= 13\%026 = 13$

C.T: 13 → n

* For P.T. t => $E(t,13) = (19+13)\%026$
$= 32\%026 = 6$

C.T: 6 → g

* For P.T. c => $E(c,13) = (2+13)\%026 = 15\%026$
$= 15$

C.T: 15 → P

* For P.T. K => $E(K,13) = (10+13)\%026 = 23\%026 = 23$

C.T 23 → X

* For P.T. 'i' => $E(i,13) = (8+13)\%026 = 21\%026 = 21$

C.T. 21 → V

19DCS093

=> For P.T. S => E(S,13) = (18+13)%26 = 5

C.T: 5 → f

=> For P.T. O => E(O,13) = (14+13)%26 = 27%26 = 1

C.T: 1 → b

=> For P.T. d => E(d,13) = (3+13)%26 = 16

C.T.: 16 → Q

=> For P.T y => E(y,13) = (24+13)%26 = 11

C.T. => 11 → L

=> For plain text: attack is today;

obtained cipher text is:-

nggapx vf gbanl

1901CS093

(4) Plain Text: welcome to the world of cryptography

Key: 7 ; Algo: Shift Cipher

⇒ logic of encryption: $(P+K)\%26 = C.T.$

⇒ For P.T. → w ⇒ 22 ; Encryption: $(22+7)\%26 = 3$

C.T. 3 → D ⇒

⇒ For P.T. e → 4 ; E: $(4+7)\%26 = 11$

C.T.: 11 → L (l)

⇒ For P.T. l → 11 ; E: $(11+7)\%26 = 18$

C.T 18 → S

⇒ For P.T. c → 2 ; E: $(2+7)\%26 = 9$

C.T. 9 → J

⇒ For P.T. o → 14 ; E: $(14+7)\%26 = 21$

C.T.: 21 → V

⇒ For P.T: m → 12 ; E: $(12+7)\%26 = 19$

C.T. 19 → T

⇒ For P.T. t → 19 ; E: $(19+7)\%26 = 0$

C.T. 0 → a

18

④ 1905093

=> P.T. : h → 7; E : (7+7) %26 = 14
C.T. 14 → O

=> P.T : y → 17; E = (17+7) %26 = 24
C.T. : 24 → Y

=> P.T. d → 3; E : (3+7) %26 = 10
C.T. 10 → K

=> P.T. f → 5; E : (5+7) %26 = 12
C.T. 11 → M

=> P.T. Y → 24 : E (24+7) %26 = 5.
C.T. : 5 → F

=> P.T : p → 15; E : (15+7) %26 = 22
C.T. : 22 → W

=> P.T. g → 6; E : (6+7) %26 = 13
C.T : 13 → N

=> P.T. a → 0; E : (0+7) %26 = 7
C.T : h

=> P.T. h → 7; E = (7+7) %26 = 14
C.T 14 → O

=> P.T. : welcome to the world of cryptography

=> obtained C.T :-
dlsjvtl av aol dvysk vm jyfwavnyhwof

19DCS098

(7) Plain Text: - check your internet connectivity
Key: covid
Algo.: Playfair

=> Firstly, we will construct 5x5 matrix and will fill up the cells with the help of the key

c	o	v	i/j	d
a	b	e	f	g
h	k	l	m	n
p	q	r	s	t
u	w	x	y	z

=> Now, we will convert the plain text in digraph

19ORS0098

GABBAR Page No. Date 20

=> ch ec ky ou ri nt er ne tc on ne ct iv it yx

=> For ch, (Same column)
c -> a
h -> p

=> For ec, (case 3)
e -> a
c -> v

=> For ky (case 3)
k -> m
y -> w

=> For ou, (case 3)
o -> c
u -> w

=> For ri, (case 3)
r -> s
i -> v

=> For nt, (Same column)
n -> t
t -> z

=> For er, (Same column)
e -> d
r -> x

For ne, (case 3)
n -> l
e -> g

For tc, (case 3)
t -> p
c -> d

for on (case 3)
o -> d
n -> k

for ne (case 3)
n -> l, e -> g

for ct, (case 3)
c -> d, t -> p

for iv (same row)
i -> d, v -> i

for it, (case 3)
i -> d, t -> s

for yx (same row)
y -> z, x -> y

P.T => check your internet connectivity
obtained C.T => apavmwcwsvtzlxlgpddklgdlpdidszy

19DCS093

(10) Plain text: meet me at tajmahal on the valentine day

Rows = 4; Algo: Rail fence

⇒ We will arrange the plain text in the diagonal form with depth 4

m		m		t	a	o	e	e	n	y
	e		e	a	h	n	v	n	e	
		e		a		t		t		
			t		j		a		d	
				m		h		i		a
					l		l		a	

⇒ From the above, we will derive the Cipher text;

C.T = mmtaoeenyeeahnvneeajatatdttmlnlia

1901CS048

Q-2 Calculate the plain text for following :-

(2) C.T = VQEVFQKPEAOQIOAJSQNECY
PLELPQNOLPQSIANIPANYQLPQKE
OFZAOQLPQENQUKPEZE

Key = 17 , Algorithm = multiplicative

=> Firstly, for decryption, we will require K^{-1}.
=> First, we will check if K^{-1} exists.

If gcd(17, 26) == 1 , then K^{-1} exists

=> As gcd(17, 26) = 1; K^{-1} will exists.

=> We will find K^{-1}, with the help of formula $\boxed{t = t_1 - (q \times t_2)}$

q	r_1	r_2	r	t_1	t_2	t
1	26	17	9	0	1	-1
1	17	9	8	1	-1	2
1	9	8	1	-1	2	-3
8	8	1	0	2	-3	26
	1	0		-3	26	

Now, -3 cannot be possible

∴ 26 - 3 = 23 is multiplicative inverse.

19DCS098

=> For C.T : V → 21; P.T => (21×23) %026 = 15
For P.T : 15 → P

=> For C.T : Q → 16; P.T => (16×23) %026 = 4 → E

=> C.T. : E → 4; P.T = (4×23) %026 = 14 → O

=> For C.T. F → 5; P.T => (5×23) %026 = 11 → L

=> For C.T. Q → 16; P.T => (16×23) %026 = 4 → E

=> For C.T. K → 10; P.T => (10×23) %026 = 22 → W

=> For C.T. P → 15; P.T => (15×23) %026 = 7 → H

=> For C.T A → 0; P.T => (0×23) %026 = 0 → A

=> For C.T. O → 14, P.T => (14×23) %026 = 10 → K

=> For C.T. D → 3; P.T => (3×23) %026 = 17 → R

=> For C.T J → 9; P.T => (9×23) %026 = 25 → Z

=> For C.T S → 18, P.T => (18×23) %026 = 24 → Y

=> For. N → 13, P.T => (13×23) %026 = 13 → N

=> For C → 2; P.T => (2×23) %026 = 20 → U

=> For Y → 24; P.T => (24×23) %026 = 6 → G

=> For L → 11; P.T => (11×23) %026 = 19 → T

14DCS098

=> For C.T. G → 6 ; P.T = (6×23) % 26 = [8 → I]

=> For C.T. U → 20 ; P.T = (20×23) % 26 = [18 → S]

=> For C.T. Z → 25 ; P.T = (25×23) % 26 = [3 → D]

=> Obtained decrypted text :->

PEOPLE WHO ARE CRAZY ENOUGH TO THINK THEY CAN CHANGE THE WORLD ARE THE ONES WHO DO

(5) C.T => GHCZEHRHGQRHEUNHYOCYUNH AMTBKC2WJ

Key => N ; Algo. => Auto Key

C.T =>	G	H	C	Z	E	H	R	H	G	Q
C's value =>	6	7	2	25	4	7	17	7	6	16
Keystream value	13	6	7	8	25	4	7	17	7	6
		19	14	14	11	19	14	3	4	2
P.T's value =>	19	14	14	11	19	12	3	4	2	14

CT ->	R	H	E	U	N	H	Y	O	C	Y	U	N	H
C's value	17	7	4	20	13	7	24	14	2	24	20	13	7
Keystream	14	3	4	2	0	20	19	14	10	4	24	0	20	19
PT's => value	3	4	0	20	19	14	10	4	24	0	20	19	14

19ORS048

C.T	A	M	T	B	K	C	L	W	J
CTvalue	0	12	19	1	10	2	11	22	9
Keyvalue	14	12	0	19	8	2	0	11	11
PTvalue	12	0	19	8	2	0	11	11	24

P.T value	19	14	14	11	19	14	3	4	2	14
P.T.	T	O	O	L	T	O	D	E	C	O

P.T value	3	4	0	20	19	14	10	4	24	0	20	19	
P.T.	D	E	A	U	T	O	K	E	Y	A	U	T	

P.Tvalue	14	12	0	19	8	2	0	11	11	24
P.T.	O	M	A	T	I	C	A	L	L	Y

Obtained Plain text =>

TOOL TO DECODE AUTOKEY AUTOMATICALLY

19DCS098

(8) C.T = BAPHYFJIXCYGYCHZHMYZ

Key = BACKUP

⇒ To make it usable, we will use bogus characters

Key = BACKUPBBB

$$Key = \begin{bmatrix} B & A & C \\ K & U & P \\ B & B & B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 1 & 1 & 1 \end{bmatrix}$$

⇒ For; Decryption; we will require K^{-1}

as $\boxed{P.T = K^{-1} . (C.T)}$

$$\Delta = 1(20-15) + 2(10-20)$$
$$= 5 + 2(-10)$$
$$= 5 - 20 = -15$$

$$\Delta = -15 \bmod 26 = 11$$

$$K^T = \begin{bmatrix} 1 & 10 & 1 \\ 0 & 20 & 1 \\ 2 & 15 & 1 \end{bmatrix}; \quad Adj(K) = \begin{bmatrix} 5 & 2 & -40 \\ 5 & -1 & 5 \\ -10 & -1 & 20 \end{bmatrix}$$

19DCS093

* Using extended Euclidean Algorithm

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	+5	-7	26
	1	0		-7	26	

$\therefore -7 \bmod 26 = 19$

$$K^{-1} = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix}$$

NOW; CT = BAP HVF JIX GCYC HZH MYZ

$$\begin{bmatrix} B \\ A \\ P \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \\ 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 5 \\ 12 \\ 24 \end{bmatrix} = \begin{bmatrix} F \\ M \\ Y \end{bmatrix}$$

Similarly, for other vertors, performing the same operation

$\therefore$ PT = FMYNIH COCWANXXERE

Q-3 (1) Plain text = YES
Cipher text = CIW

Algorithm = Shift Cipher

=> For Shift Cipher; C_i is the shift down of K characters of P_i

=> We get C by shifting y down by 4 char.

=> We get I by shifting E down by 4 characters

=> We get W by shifting S down by 4 characters.

So; **Key = 4**

=> Given Cipher text = XVIEWYWI

To get Plain text, we will simply shift down the C_i by 4 characters.

For Easy way $P_i = (C_i - 4) \bmod 26$

=> $P_X = (23-4) \bmod 26 =$ **19 → T**

=> $P_V = (21-4) \bmod 26 =$ **17 → R**

=> $P_I = (8-4) \bmod 26 =$ **4 → E**

=> $P_E = (4-4) \bmod 26 =$ **0 → A**

19015098

=> $P_W = (22-4) \bmod 26 = |18 \to S|$

=> $P_Y = (24-4) \bmod 26 = |20 \to U|$

=> $P_W = 18 \to S \mid P_I = |4 \to E|$

C.T = X V I E W Y W I

P.T = I R E A S U S E

=> The Attack we used is Know Plain text Attack & C.T & P.T were known so we found the key by mapping.

19DCS098

Ans-(4) Key = cryptography

Plaintext = ~~par~~ 19DCS098PARTHPATEL

Algorithm = Playfair Cipher

=) Here, Playfair Cipher is only for alphabet, so we will perform encryption for

DCSPARTHPATEL

=) Matrix for encryption:-

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

=) We will convert the formatted plaintext into digraphs

=) Formatted P.T in the form of digraph:-

DC SP AR TH PA TE LX

=) We will start the decryption:-

19DCS098

⇒ For DC
(same column)
D → L
C → O
∴ DC → LO

⇒ For SP
(Case: 3)
S → Q
P → T
SP → QT

⇒ For AR
(Case: 3)
A → G
R → Y
AR → GY

⇒ For TH
(Case: 3
T → P
H → B
TH → PB

⇒ For PA
(Case: 3
P → Y
A → H
PA → YH

⇒ For TE
(Case: 3)
T → R
E → K
TE → RK

⇒ For LX
(Case: 3)
L → Q
X → U
LX → QU

∴ Given Plain Text = 19DCS098 PARTH PATEL

∴ Formatted P.T = DCSPARTHPATELX

∴ Obtained Cipher Text

= LOQTGYPBYHRKQU

19DCS098

(7)

My ID: 19DCS098

$p = 19 + 98 = 117$

⇒ Now;
Total number of possible keys in affine cipher for $Z_p = p \times \phi(p)$

$\therefore p = 117$

$\phi(p) = \phi(117) = \phi(13 \times 9)$
$= \phi(13) \times \phi(3^2)$

By Eulers totient thm;

$\phi(117) = \phi(13) \times \phi(3^2)$
$= (13-1) \times (3^2 - (3)^1)$
$= (12) \times (9-3)$
$= 12 \times 6$
$= 72$

⇒ no. of keys $= 117 \times 72$
$= 8424$

(12) Elaborate various attacks on RSA algorithm

* Some Potential Attacks on RSA :-
  (1) Factorization Attack
  (2) Chosen-Ciphertext Attack
  (3) Encryption exponent Attack
  (4) Decryption exponent Attack
  (5) Plaintext Attack
  (6) Modulus Attack
  (7) Implementation Attack

* Plain Text Attack :-

⇒ Plain text Attack are divided into three categories :-
  (1) Short Message Attack
  (2) Cycling Attack
  (3) Unconcealed message attack

* Short Message Attack :-

→ In this type of attack, the assumption is that the attacker knows some blocks of plain text message.

→ If attacker knows some block of plain text, then he could try to encrypt the blocks of plain text using the information and try to convert it into cipher text.

1ad15098

GAURAV
Page No.
Date : / / 20

→ To prevent short message attack, we can use padding bits for encryption

* Cycling attack:-

→ Here, attacker assumes that the cipher text is formed using some permutation operations.

→ If the assumption becomes true, he can try the reverse process to obtain the plain text.

* Unconcealed Message Attack:-

→ When encrypted cipher text is the same as the plain text, then such attack can take place.

* Chosen Cipher text Attack:-

⇒ The attacker can find out the plain text from the cipher text using extended euclidean algorithm.

1AOCS098

* Factorization Attack:-

=> In factorization attack, the attacker impersonates the key owners.

-> With the help of the stolen data, they decrypt the sensitive data, bypass the security of the system.

-> This attack occurs on RSA cryptographic library.

-> So, attackers can have the private keys of n number of security tokens, etc.