ASSIGNMENT

SUBJECT NAME: CRYTOGRAPHY AND SECURITY IN COMPUTING

SUBJECT CODE: T18 CIT01

SEM / YEAR : 7th semester / Final year

BATCH : 2020-2024

FACULTY NAME : Dr. G. FATHIMA
Prof & HOD / CSE.

- Submitted by

NAME: SHARANJI. P

REG NO : AC20UCS120.

SEM/SEC : 7th sem / C-sec

DEPT : BE-CSE

SIGNATURE :

Assignment - I

i) Given plain text and key. find cipher text using caesar cipher.

plain text : "Havefunwithcryptography"
key : 5

soln:-

1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L
13	14	15	16	17	18	19	20	21	22	23	24
M	N	O	P	Q	R	S	T	U	V	W	X
25	26										
Y	Z										

step 1:-

plain text : "Havefunwith cryptography" and key = 5

step 2 :-

Applying the key values of 5 and for each letter can plain text shift it 5 positions to the right in the alphabet.

The obtained ciphertext is.

cvqikrjtonyxhpinbttwnd.

ii) Decrypt the monoalphabetic ciphertext Boob vojwjstjuz.

soln:-

step 1 : Given cipher text is.

Boob vojwjstjuz.

Step2: By using the Mapping table to decrypt then the each letter will be.

B - A
O - n
O - n
b - a
v - u
O - n
j - i
N - r
f - e
s - r
t - s
j - i
u - t
z - y

Step3:

Combining the decrypted values then the final plain text is

Anna University.

2. Using playfair Matrix

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

Encrypt the message "THE ENEMY MUST BE STOPPED AT ALL COSTS".

soln:-

step 1: The given plain text is the enemy must be stopped at all costs.

Step 2: split the plain text

TH EE NE MY MU ST BE
ST OP PE DA TA LL CO
ST SX

step 3: split the same letters and replace with x.

TH EE EN, EM YM US TB ES
TO PP ED AT AL LC OS TS

step 4: 'PP' pair is same split the letter again.

TH EX EN EM YM US TB ES TO
PX PE DA TA LX LC OS TS

Step 5: Encrypting the cipher text

TH → PL	TB → QF
EX → UZ	ES → RT
EN → OF	TO → ME
EM → OT	PX → QW
YM → VS	PE → TC
VS → RQ	DA → FB

TA → PF LX → TZ
LC → HE OS → RM
TS → MT

Step 6: the final cipher text is,

PL UZ OF OT VS RQ QF
RT ME QU TC FB PF IZ HC
RM MT.

3. Using vigenere cipher encrypt the word "Cryptography" using key "College"

Step 1: Given plain text: Cryptography
key: COLLEGE COLLE

Step 2: Converting both key and Plain text into number

A = 0
B = 1 &
so on.

Plain text: 2 17 24 19 16 . 21 6 15
key 2 14 11 6 4 6 2 14
6 19 15 24
1 16 4 6

Step 3:
Add the corresponding numbers

Ciphertext: 4 5 2 25 20 18 , 3 11
4 21

Step 4: Convert the number in ciphertext back to letters then the ciphertext is.

EFCZUBIDLECV.

4 Encrypt the message "Meet me at the usual place at ten pm" by using hill cipher with key [9 4] [5 7] show the calculation for corresponding decryption of ciphertext to recover the original plain text.

Soln

Step 1: Plain text : Meet me at the usual place at ten PM.

Key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Step 2: Encrypt the plain text.

$$Me = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{pmatrix} 20 \\ 10 \end{pmatrix}$$

$$et = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 8 \\ 23 \end{bmatrix}$$

$$me = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 20 \\ 10 \end{bmatrix}$$

$$at = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{pmatrix} 24 \\ 3 \end{pmatrix}$$

$$th = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 17 \\ 14 \end{bmatrix}$$

$$qu = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 20 \end{bmatrix} \bmod 26$$

$$= \begin{pmatrix} 12 \\ 4 \end{pmatrix}$$

$$sv = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 20 \end{bmatrix} \bmod 26$$

$$= \begin{pmatrix} 8 \\ 22 \end{pmatrix}$$

$$at = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 \\ 25 \end{bmatrix}$$

$$pu = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 23 \\ 22 \end{bmatrix}$$

$$at = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$ea = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 10 \\ 20 \end{bmatrix}$$

$$tt = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 13 \\ 20 \end{bmatrix}$$

$$en = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 13 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 7 \end{bmatrix}$$

$$Pm = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 12 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 13 \\ 14 \end{bmatrix}$$

The cipher text is

UKIXUKYDRDMEIWSZKWIOKUNUAHNO

<u>Step3</u> : Decrypt the cipher text

$$P = k^{-1} e \bmod 26$$

$$= k^{-1} kP = P$$

We can use 23, $\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$

$$23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 4 \end{bmatrix} \Rightarrow ME$$

$$23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \begin{bmatrix} 8 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 19 \end{bmatrix} \Rightarrow ET$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}20\\10\end{bmatrix} \bmod 26 = \begin{bmatrix}12\\4\end{bmatrix} \Rightarrow ME$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}24\\3\end{bmatrix} \bmod 26 = \begin{bmatrix}0\\9\end{bmatrix} \Rightarrow AT$$

$$23\begin{bmatrix}9 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}17\\14\end{bmatrix} \bmod 26 = \begin{bmatrix}17\\7\end{bmatrix} \Rightarrow TM$$

$$23\begin{bmatrix}9 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}12\\4\end{bmatrix} \bmod 26 = \begin{bmatrix}3\\17\end{bmatrix} \Rightarrow EU$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}6\\22\end{bmatrix} \bmod 26 = \begin{bmatrix}18\\20\end{bmatrix} \Rightarrow SU$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}18\\25\end{bmatrix} \bmod 26 = \begin{bmatrix}12\\4\end{bmatrix} \Rightarrow AE$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}13\\23\end{bmatrix} \bmod 26 = \begin{bmatrix}12\\4\end{bmatrix} \Rightarrow PL$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}8\\14\end{bmatrix} \bmod 26 = \begin{bmatrix}0\\2\end{bmatrix} \Rightarrow AC$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}10\\20\end{bmatrix} \bmod 26 = \begin{bmatrix}4\\0\end{bmatrix} \Rightarrow EA$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}13\\20\end{bmatrix} \bmod 26 = \begin{bmatrix}17\\14\end{bmatrix} \Rightarrow TO$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}0\\7\end{bmatrix} \bmod 26 = \begin{bmatrix}4\\13\end{bmatrix} \Rightarrow EN$$

$$23\begin{bmatrix}7 & -4\\ -5 & 9\end{bmatrix}\begin{bmatrix}13\\14\end{bmatrix} \text{Mod } 26 = \begin{bmatrix}15\\12\end{bmatrix} \Rightarrow PM$$

The final plain text is meet me at the usual place at ten PM.

5. Given the key "MONARCHY" apply playfair technique to plain text "FACTIONALISM" to ensure confidentiality at the destination, decrypt the cipher text and establish authentication.

soln

Step1:

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

key : MONARCHY

Plaintext : FACTIONALISM.

Step2 ; split the plain text

FA CT IO NA LI SM

FA → IO

CT → DL

IO → FA

NA → AR

LI → SE

SM → LA.

Step 3: The final cipher text is

IODLFAARSELA.

6. Encipher the Message "I CAME SAW I CONQUERED" with a Rail-Fence technique of depth & 3.

Soln

Depth 2

I		A		E		S		W		C		N		U		R	
	C		M		I		A		I		O		Q		E		E

the encrypted cipher text is

IA ESWCNURDCMIAIOQEE.

Depth 3

I				E				W				N				R	
	C		M		I		A		I		O		Q		E		E
		A				S				C				U			

The encrypted cipher text is

I E W N R C M I A I O Q E E A S C U

7. Find the cipher text for the message "EASY TO ENCRYPT BUT DIFFICULT TO DECRYPT" using the key 4231657 using columnar transposition technique.

Soln

4 2 3 1 6 5 7 → key

E	A	S	Y	T	O	E
N	C	R	Y	P	T	B
U	T	D	I	F	F	I
C	U	L	T	T	O	D
E	C	R	Y	P	T	Z

The cipher text is,

YYITYACTUCSRDLRENUCEOTTOP
TPFTPEBIDZ.

step2:

←	2	3	1	6	5	7 → key
Y	Y	I	T	Y	A	C
T	U	C	S	R	D	L
R	E	N	U	C	E	O
T	T	O	T	T	P	F
T	P	E	B	I	D	Z

The cipher text is,

TSUTBYUEFPIC NOEYIRTTABEPD
YRCTICLOFZ.

→ Rewrite the text column wise according to the key number.

8. Find gcd

i) gcd (1970, 1066).

= gcd (1066, 1970 mod 1066)

= gcd (1066, 904)

= gcd (904, 1066 mod 904)

= gcd (904, 162)

= gcd (162, 904 mod 162)

= gcd (162, 94)

= gcd (94, 162 mod 94)

$= \gcd(94, 68)$

$= \gcd(68, 94 \bmod 68)$

$= \gcd(68, 26)$

$= \gcd(26, 68 \bmod 26)$

$= \gcd(26, 16)$

$= \gcd(16, 26 \bmod 16)$

$= \gcd(16, 10)$

$= \gcd(10, 16 \bmod 10)$

$= \gcd(10, 6)$

$= \gcd(6, 10 \bmod 6)$

$= \gcd(6, 4)$

$= \gcd(4, 6 \bmod 4)$

$= \gcd(4, 02)$

$= \gcd(2, 4 \bmod 2)$

$= \gcd(2, 2)$

$\therefore$ The final gcd of 1970 & 1066 is 2.

ii) gcd (2740 and 1760).

$= \gcd(1760, 2740 \bmod 1760)$

$= \gcd(1760, 980)$

$= \gcd(980, 1760 \bmod 980)$

$= \gcd(980, 780)$

$= \gcd(780, 980 \bmod 780)$

$= \gcd(780, 200)$

$= \gcd(200, 780 \bmod 200)$

$= \gcd(200, 180)$

$= \gcd(180, 200 \bmod 180)$

$= \gcd(180, 20)$

$= \gcd(20, 180 \bmod 20)$

$= \gcd(20, 0)$

$\therefore$ The final GCD is 20.

(iii) $\gcd(24140, 16762)$

$= \gcd(16762, 24140 \bmod 16762)$

$= \gcd(16762, 7378)$

$= \gcd(7378, 16762 \bmod 7378)$

$= \gcd(7378, 2006)$

$= \gcd(2006, 7378 \bmod 2006)$

$= \gcd(2006, 1360)$

$= \gcd(1360, 2006 \bmod 1360)$

$= \gcd(1360, 646)$

$= \gcd(646, 1360 \bmod 646)$

$= \gcd(646, 68)$

$= \gcd(68, 646 \bmod 68)$

$= \gcd(68, 34)$

$= \gcd(34, 0)$

Hence, the final GCD of 24140 & 16762 is 34.

9. Using extended euclid's algorithm find the multiplicative inverse of 15 with respect to mod 29.

Q	A	B	R	T_1	T_2	T
1	29	15	14	0	1	-1
1	15	1	1	1	-1	2
14	14	1	0	-1	2	-42
X	1	0	X	1	-42	X

The above table is the extended euclid's algorithm.

step 1: We take Q, A, B, R, T1, T2, T

Q → Quotient

R → Remainder

Initially T1 & T2 value is 0 & 1

step 2: 29 mod 15 gives the remainder 14 and Quotient is 1.

Step3: T is calculated using

$T_1 - T_2 = T$

Step4: Shift the values in right side of the column.

Step 5: Again do the steps until we can't find the remainder 8 as quotient.

Step 6: Once we reach the state stop the algorithm, The final answer is 11.

∴ Multiplicative inverse of 15 with respect to mod 29 is 2.

10 Does 561 is prime or not? Test for primality of 561 using Miller-Rabin algorithm?

Soln

Given $n = 561$

Step1: $n-1 = 2^k \times m$

$560 = 2^4 \times 35$

So, $k=4$, $m=35$

Step2: Choosing a value

$a=2$, $1<2<560$

a should be greater than 1 &

less than $n-1$

Step 3: Compute $b_0 = a^m \pmod{n}$

$$b_0 = a^m \pmod{n}.$$

$$b_0 = 2^{35} \pmod{561}$$

$$= 263$$

is $b_0 = \pm 1 \pmod{561}$

so calculate b_1

$$b_1 = b_0^2 \pmod{n}$$

$$b_1 = 263^2 \pmod{561}$$

$$b_1 = 166$$

is $b_1 = \pm 1 \pmod{561}$

$$b_2 = b_1^2 \pmod{n}.$$

$$b_2 = 166^2 \pmod{561}$$

$$b_2 = 67$$

is $b_2 = \pm 1 \pmod{561}$

$$b_3 = b_2^2 \pmod{n}$$

$$b_3 = b_7^2 \pmod{561}$$

$b_3 = 1 \Rightarrow$ composite

561 is composite so it is not a prime number.

(11) Using formats theorem solve $3^{201} \bmod 11$.

soln

Given $p = 11$ and $a = 3$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$3^{10} \equiv 1 \bmod 11$$

$$3^{201} \equiv (3^{10})^{20} \times 3 = 3 \bmod 11$$

the final answer is 3.

(12) Determine $\phi(41)$, $\phi(27)$, $\phi(231)$, $\phi(440)$.

step 1: Using euler's totient function

$\phi(41) = 41$ is a prime

$= 41 - 1$

$= 40$

$\phi(41) = 40$

$\phi(27) = 3^3$

$= 27 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{3}\right)$

$= 18$

$\phi(231) = 3 \times 7 \times 11$

$= 231 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{7}\right) \times \left(1 - \frac{1}{11}\right)$

$= 120$

$\phi(440) = 2^3 \times 5 \times 11$

$= 440 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{11}\right)$

$= 320$

13 User A and B use the diffie-hellman key exchange technique with a common prime $q = 71$ & primitive root $\alpha = 7$.

i) If user A has private key $X_A = 5$, What is A's public key Y_A?

Let $q = 71$, $\alpha = 7$

User A

$X_A = 5$

$Y_A = 7^5 \bmod 71$

key which is symmetric & it is not symmetric because both User A and User B independently compute the coefficient shared secret key (k) using the other party's public key and their own private key

$k = (Y_B \wedge X_A) \% q = (Y_A \times Y_B) \% q$

Shared secret key

∴ The shared secret key at sender $A = \begin{pmatrix} \text{Public key} \\ \text{of } B \end{pmatrix} \times \begin{pmatrix} \text{Private key} \\ \text{of } A \bmod q \end{pmatrix}$

$= 4 \times 5 \bmod 71$

$= 1024 \bmod 71$

$= 30.$

The shared secret key at receiver

$$B = \left(\begin{matrix}\text{Public key} \\ \text{of } A\end{matrix}\right) \times \left(\begin{matrix}\text{Private key of} \\ B \bmod q\end{matrix}\right)$$

$= 51 \times 12 \bmod 71$

$= 64.$

The shared secret keys are different for user A and user B so it is not a symmetric key.

$= 16807 \bmod 11$

$Y_A = 51$

ii) If user B has private key $X_B = 12$, what is B's public key Y_B?

User B,

$X_B = 12$

$Y_B = 7^{12} \bmod 71$

$= 7^6 + 7^6 \bmod 71$

$= 117647 + 117649 \bmod 71$

$= 235298 \bmod 71$

$= 4$

i) Is the key symmetric? If so justify it?

The diffie hellman key exchange technique establishes a shared secret key.

14 Perform encryption and decryption using RSA algorithm $p=3$, $q=11$, $m=5$.

soln

Given:

$n = p \times q$, $e = 7$

$n = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1)$

$= 2 \times 10$

$= 20$

$\gcd(e, \phi(n)) = (20, 7) = 1$

$de = 1 \mod (\phi(n))$

$d7 = 1 \mod 20$

$d = 3$

Public key $k_u = \{e, n\} = \{7, 33\}$

Private key $k_r = \{d, n\} = \{3, 33\}$

encryption

$c = m^e \mod n$

$m = 5$

$= 5^7 \mod 33$

$c = 14$

Decryption

$m = c^d \mod n$

$= 14^3 \mod 33$

$= 5$

In a public-key System using RSA, you intercept the ciphertext $c=10$ sent to a user whose public key is $e=5$, $n=35$. What is the plaintext m?

soln

Given

$e=5, \quad n=35$

we need to calculate d to decrypt the ciphertext

$c=10$

prime factors of n.

$n=35 \Rightarrow 5 \times 7$

Calculate euler's totient $\phi(n)$

$$\phi(n) = (p-1)(q-1)$$
$$= (5-1)(7-1)$$
$$= (4)(6)$$
$$= 24$$

Calculate private key exponent (d).

$$5d \equiv 1 \pmod{24}$$
$$d \equiv 5 \cdot 5$$
$$\equiv 25$$
$$\equiv 1 \pmod{24}$$
$$d = 5$$

decrypt the ciphertext

$m = c^{\wedge} d \bmod n$

$= 10^{\wedge} 5 \bmod 35$

$= 100000 \bmod 35$

$m = 5$

The plain text m is 5.

16. Consider an elgamal schema with a common prime $q = 71$ and a primitive root $\alpha = 7$.

a) If B has public key $Y_B = 3$ and A choose the random integer $k = 2$, what is the cipher text of $M = 30$?

Given;-

$d = 7$

$q = 71$

$M = 30$

$Y_B = 3$

$k = 2$

$c_1 = \alpha^k \bmod q$

$c_1 = (M + Y_B^k) \bmod q$

$= 7^2 \bmod 71$

$= 49 \bmod 71$

$c_1 = 49$ //

$c_2 = (30 + 3^2) \bmod 71$

$= 270 \bmod 71$

$= 25$ //

Hence, the ciphertext $M = 30$ with these values $(49, 25)$.

ii) If A now choose a different value of k so that the encoding of $M = 30$ is $c = (59, c_2)$ what is the integer c_2.

Given:

$c1 = 59$

$M = 30$

$Y_B = 3$

Determine the value of k.

$k = \log_7 (c_1) \bmod q$

$k = \log_7 (59) \bmod q$.

Calculate the value of k.

$k = 3$

$c_2 = (M * Y_B)^k \bmod q$

$= (30 * 3^3) \bmod 71$

$= 270 \bmod 71$

$= 47$