NAME: Marcena Fernandes ROLL NO: 8669 CLASS: TE IT

CNS ASSIGNMENT - 1

1 Encrypt the message "we are all together" using a double transposition cipher with 4 rows and 4 columns, using row permutation (1,2,3,4) → (2,4,1,3) and column permutation (1,2,3,4) → (3,1,2,4)

→ Solutions:

M = WE ARE ALL TOGETHER

	1	2	3	4
1	W	E	A	R
2	E	A	L	L
3	T	O	G	E
4	T	H	E	R

Row (1,2,3,4) → (2,4,1,3)

	1	2	3	4
1	E	A	L	L
2	T	H	E	R
3	W	E	A	R
4	T	O	G	E

Column (1,2,3,4) → (3,1,2,4)

	1	2	3	4
1	L	E	A	L
2	E	T	H	R
3	A	W	E	R
4	G	T	O	E

Cipher : LEAL ETHR AWER GTOE

Alice's RSA public key is $(N, e) = (33, 3)$ and her private $d = 7$

a. If Bob encrypts the message $M = 19$ for Alice, what is the ciphertext C? Show how Alice can decrypt ciphertext to get the message

→ Solution:

$N = 33 \quad e = 3 \quad d = 7 \quad M = 19$

Encryption : Cipher $(C) = M^e \text{ Mod } N$

$= 19^3 \text{ Mod } 33$

$= 28$

Decryption : Message $(M) = C^d \text{ Mod } N$

$= 28^7 \text{ Mod } 33$

$= \boxed{19}$

b Let S be the result when Alice digitally signs the message $M = 25$. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature. Show that in this case signature verification succeeds.

→ Solution:

Alice will use private key d for digital signature

$M = 25 \quad d = 7 \quad N = 33$

$S = M^d \text{ Mod } N$

$= 25^7 \text{ Mod } 33$

$= 31$

When Bob recieves M and S, it will use Alice's public key to decipher S. If the deciphered message is equal to M, the signature is verified.

Deciphered Message $= S^e \text{ Mod } N$

$= 31^3 \text{ Mod } 33$

$= \boxed{25} = M$

Thus it is verified.

3 Given the super increasing tuple = {7, 11, 23, 43, 87, 173, 357}, $r = 41$ and modulus $n = 1001$, encrypt and decrypt the letter 'a' using knapsack cryptosystem. Use [7 6 5 1 2 3 4] as permutation table

→ Solution:

$W = \{7, 11, 23, 43, 87, 173, 357\}$

$n = 1001 \quad r = 41$

Public key sequence = $w \times r \bmod n$

$= \{287, 451, 943, 762, 564, 86, 623\}$

$a = 1$

Permutation Table [7 6 5 1 2 3 4]

0 0 0 1 0 0 0

Cipher = $0 \times 287 + 0 \times 451 + 0 \times 943 + 1 \times 762 + 0 \times 564 + 0 \times 86 + 0 \times 623$

$= 762$

Encrypted $a = 7$

Decryption:

$Sum = c \times r^{-1} \bmod n$

$[r^{-1} : 41 \times x \bmod 1001 = 1]$

$\therefore r^{-1} = 293$

$Sum = 762 \times 293 \bmod 1001$

$= 43 = \boxed{43 \times 1}$

$W = \{7, 11, 23, 43, 87, 173, 357\}$

For 43 : 0 0 0 1 0 0 0

Comparing to permutation table

[7 6 5 1 2 3 4]

0 0 0 1 0 0 0

$= 1 = a$

Thus, decrypted.

4 Encrypt the message "this is an exercise" using the following cipher. Ignore the space between words. Decrypt to get the plaintext.

- Additive cipher with key = 20
- Multiplicative cipher with key = 15
- Affine cipher with key (15, 20)

→ Solution:

M = THIS IS AN EXERCISE

- Additive cipher with key = 20

Formula : M + key mod 26

M = 19 7 8 18 8 18 0 13 4 23 4 17 28 18 4

Message : M + 20 Mod 26

Cipher 13 1 2 12 2 12 20 7 24 17 24 11 22 2 12 24

Cipher Text : NBCM CMUH YRYL WCMY

Decryption:

Formula : M - key mod 26

M = 13 1 2 12 2 12 20 7 24 17 24 11 22 2 12 24

Message : M - 20 Mod 26

Cipher 19 7 8 18 8 18 0 13 4 23 4 17 28 18 4

Text : THIS IS AN EXERCISE.

- Multiplicative cipher with key = 15

Inverse $15 \times x \bmod 26 = 1$

$\therefore x = 7$

Encryption:

M = 19 7 8 18 8 18 0 13 4 23 4 17 2 8 18 4

× 15 mod 26

Cipher = 25 1 16 10 16 10 0 13 8 7 8 21 4 16 10 8

Cipher text = ZBQK QKAN IHIV EQKI

Decryption:

Formula = M × 7 Mod 26

→ 19 7 8 18 8 18 0 13 4 23 4 17 2 8 18 4

Message: THIS IS AN EXERCISE.

- Affine cipher with key (15, 20)

Inverse 20, x

$15 \times x \bmod 26 = 1$

$x = 7$

Formula for encryption = M × 15 + 20 mod 26

C = 19 7 8 18 8 18 0 13 4 23 4 17 2 8 18 4

× 15 + 20 mod 26

Cipher = 19 21 10 4 10 4 20 7 2 1 2 15 24 10 4 2

Cipher text: TVKE KEUH CBCP YKEW

Decryption:

Formula: M − 20 × 7 mod 26

M: 19 7 8 18 8 18 0 13 4 23 4 17 2 8 18 4

Text: THIS IS AN EXERCISE

5. Encrypt the message "This house is being sold tonight" using the following ciphers. Ingnore the space between words. Decrypt to get the plaintext.
- Vingenere cipher with key = "dollars"
- Autokey cipher with key = 7

→ Solution:

M = THIS HOUSE IS BEING SOLD TONIGHT.

- Vingenere cipher with key = "dollars"
= 3 14 11 11 0 17 18

M: THIS HOUSE IS BEING

C = 19 7 8 18 7 14 20 18 4 8 18 1 4 8 13 6
+ 3 14 11 11 0 17 18 3 14 11 11 0 17 18 3 14 (mod 26)

Cipher = 22 21 19 3 7 5 12 21 18 19 3 1 21 0 16 20

M = SOLD TONIGHT

C = 18 14 11 3 19 14 13 8 6 7 19
3 14 11 11 0 17 18 3 14 11 11 (mod 26)

Cipher = 3 25 11 20 11 17 1 19 17 7 10

Cipher text: WVTD HFMV STDB VAQU DZLU
LRBT RHK

- Autokey cipher with key = 7

Autokey = HTHISHOUSEISBEINGSOLDTONIGHT

P:	19	7	8	18	7	14	20	18	4	18	1	4	8	13	6	
+	7	19	7	8	18	7	14	20	18	4	18	1	4	8	13	
C =	0	0	15	0	0	21	8	12	22	12	0	19	5	12	21	19

P:	18	14	11	3	19	14	13	8	6	7	19
+	6	18	14	11	3	19	14	13	8	6	7
C =	24	6	25	14	22	7	1	21	14	13	0

Cipher Text: AAPA AVIM WMAT FMVT YGZO WHBV ONA

6. Use the playfair cipher to encipher the message "the key is hidden under the door pad". The ~~secret~~ secret key can be made by filling the first and part of second row with word "guidance" and filling the rest of matrix with rest of the alphabets.

→ Solution:

Playfair Matrix :

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

① Pairs: TH EK EY IS HI DX DE NU ND ER

Cipher: PO CL BX DR LG IY IB CG BG LX

② Pairs: TH ED OX OR PA DX

Cipher: PO BI LZ LT TG IY

7. Use the hill cipher to encipher message. "We live in insecure world" Use the key
$k = \{03\ 02,\ 05\ 07\}$

→ Solution:

M = WE LIVE IN INSECURE WORLD.

$k = \begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix}$

Pairs:	WE	LI	VE	IN	IN	SE	CU	RE	WO	RL	DX
	22,4	12,18	21,4	8,13	8,13	18,4	2,20	17,4	22,14	17,11	3,23

① $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 22 \\ 4 \end{matrix} = \begin{matrix} 74 \\ 138 \end{matrix}$ mod 26 = 22 = W
mod 26 = 8 = I

② $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 12 \\ 18 \end{matrix} = \begin{matrix} 52 \\ 116 \end{matrix}$ mod 26 = 0 = A
mod 26 = 12 = M

③ $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 21 \\ 4 \end{matrix} = \begin{matrix} 71 \\ 133 \end{matrix}$ mod 26 = 19 = T
mod 26 = 3 = D

④ $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 8 \\ 13 \end{matrix} = \begin{matrix} 48 \\ 131 \end{matrix}$ mod 26 = 22 = W
mod 26 = 1 = B

⑤ $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 8 \\ 13 \end{matrix} = \begin{matrix} 48 \\ 131 \end{matrix}$ mod 26 = 22 = W
mod 26 = 1 = B

⑥ $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 18 \\ 4 \end{matrix} = \begin{matrix} 62 \\ 118 \end{matrix}$ mod 26 = 10 = K
mod 26 = 14 = O

⑦ $\begin{matrix} 3 & 2 \\ 5 & 7 \end{matrix} \times \begin{matrix} 2 \\ 20 \end{matrix} = \begin{matrix} 46 \\ 150 \end{matrix}$ mod 26 = 20 = U
mod 26 = 20 = U

⑧ $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 59 \\ 113 \end{bmatrix}$ mod 26 = 7 = H
mod 26 = 9 = J

⑨ $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 22 \\ 14 \end{bmatrix} = \begin{bmatrix} 74 \\ 208 \end{bmatrix}$ mod 26 = 22 = W
mod 26 = 0 = A

⑩ $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 17 \\ 11 \end{bmatrix} = \begin{bmatrix} 73 \\ 162 \end{bmatrix}$ mod 26 = 21 = V
mod 26 = 6 = G

⑪ $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 3 \\ 23 \end{bmatrix} = \begin{bmatrix} 55 \\ 176 \end{bmatrix}$ mod 26 = 3 = D
mod 26 = 20 = U