



Security of Computer and Networks

asaad.nayyef@uomus.edu.iq



Vernam Cipher: type of substitution cipher used for data encryption. The Vernam cipher was devised in 1918 by Gilbert S. Vernam.

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ex1: Try to encrypt the following plaintext using Vernam cipher system:

Plaintext = VERNAMCIPHER

Key= 76 48 16 82 44 3 58 11 60 5 48 88

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Letter Value	21	4	17	13	0	12	2	8	15	7	4	17
Key	76	48	16	82	44	3	58	11	60	5	48	88
Sum +	97	52	33	95	44	15	60	19	75	12	52	105
Mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Cipher	T	A	H	R	S	P	I	T	X	M	A	B



Security of Computer and Networks

asaad.nayyef@uomus.edu.iq



Ex2: Try to decrypt the following ciphertext using Vernam cipher system:

Ciphertext= t a h r s p i t x m a b

Cipher	T	A	H	R	S	P	I	T	X	M	A	B
Letter Value	19	0	7	17	18	15	8	19	23	12	0	1
Key	76	48	16	82	44	3	58	11	60	5	48	88
Sub -	78	52	26	104	52	26	78	26	78	26	52	104
	76	48	16	82	44	3	58	11	60	5	48	88
Sum +	2	4	10	22	8	23	20	15	18	21	4	16
	19	0	7	17	18	15	8	19	23	12	0	1
Mod 26	21	4	17	39	26	38	28	34	41	33	4	17
	21	4	17	13	0	12	2	8	15	7	4	17
Plaintext	V	E	R	N	A	M	C	I	P	H	E	R