Network Security

Homework 1

CHANG LIU

chang.liu@jhu.edu

Feb. 11, 2012

1. **plaintext: 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**
   ciphertext: m n b v c x z a s d f g h j k l p o I u y t r e w q

Solution

(a) Encode the message “This is an easy problem.”

Uasi si mj cmqw lokngch

(b) Decode the message “rmij u uamu xyj.”

wasn t that fun

2. ### Solution

(a)

Original	10100000 10100000 10100000 10100000 10100000 10100000 10100000 10100000
Output	00000101 00000101 00000101 00000101 00000101 00000101 00000101 00000101

(b)

Original	10100000 10100000 10100000 10100000 10100000 10100000 10100000 10100001
Output	00000101 00000101 00000101 00000101 00000101 00000101 00000101 10000101

(c)

Repeat part (a) again:

Original	10100000 10100000 10100000 10100000 10100000 10100000 10100000 10100000
Output	10100000 10100000 10100000 10100000 10100000 10100000 10100000 10100000

Repeat part (b) again:

Original	10100000 10100000 10100000 10100000 10100000 10100000 10100000 10100001
Output	10100001 10100000 10100000 10100000 10100000 10100000 10100000 10100000

3. ### Solution

Consider the 3 – bit block cipher table as shown on slide 9 of class notes. Suppose the plaintext is 100100100.

(a) Initially assume that CBC is not used. What is the resulting ciphertext?

011 011 011

(b) Suppose Trudy sniffs the ciphertext. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn’t know the specific cipher), what she can surmise?

She can surmise that the 3-bit blocks which has the same value in the ciphertext, will also have the same value after decrypt.

(c) Now suppose that CBC is used with initial Vector IV=111. What is the resulting ciphertext?

Plaintext 100 100 100

IV = C(0) = 111

$$c(1) = K_s(m(1) \oplus c(0)) = K_s(100 \oplus 111) = K_s(011) = 100$$
$$c(2) = K_s(m(2) \oplus c(1)) = K_s(100 \oplus 100) = K_s(000) = 110$$
$$c(3) = K_s(m(3) \oplus c(2)) = K_s(100 \oplus 110) = K_s(010) = 101$$

Receiver

$$s(1) = (m(1) \oplus c(0)) = (100 \oplus 111) = 011$$
$$s(2) = (m(2) \oplus c(1)) = (100 \oplus 100) = 000$$
$$s(3) = (m(3) \oplus c(2)) = (100 \oplus 110) = 010$$

Thus, the ciphertext is 011 000 010

4. Suluton

(a) Using Vigenere cipher, encrypt word MILLENNIUM using the key YTWOK.

Key:	Y	T	W	O	K	Y	T	W	O	K
Plaintext:	M	I	L	L	E	N	N	I	U	M
Ciphertext:	K	B	H	Z	O	L	G	E	I	W

(b) Using Vigenere cipher, decrypt word FFFLB CVFX encrypted using the key ZORRO.

Key:	Z	O	R	R	O	Z	O	R	R
Ciphertext:	F	F	F	L	B	C	V	F	X
Plaintext:	G	R	O	U	N	D	H	O	G

5. Solution

Encryption:

Message = $\begin{vmatrix} S \\ T \\ O \end{vmatrix}, \begin{vmatrix} P \\ P \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 19 \\ 14 \end{vmatrix}, \begin{vmatrix} 15 \\ 15 \\ 0 \end{vmatrix}$

$$Key = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$$

Then we do the encryption:

$$\begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}\begin{pmatrix} 18 & 15 \\ 19 & 15 \\ 14 & 0 \end{pmatrix} = \begin{pmatrix} 502 & 195 \\ 877 & 420 \\ 507 & 405 \end{pmatrix} = \begin{pmatrix} 8 & 13 \\ 19 & 4 \\ 13 & 15 \end{pmatrix} = \begin{pmatrix} I & N \\ T & E \\ N & P \end{pmatrix}$$

Thus the ciphertext is: **ITN NEP**

Dectryption:

$$|Key| = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix} = (11*23*1 + 20*2*25 + 5*7*19 - 19*23*20 - 1*2*5 - 11*25*7) \neq 0$$

thus Key^{-1} exist, and we calculate the Key^{-1}:

$$Key^{-1} = \frac{1}{|Key|} Key* = \begin{pmatrix} 18 & 15 \\ 19 & 15 \\ 14 & 0 \end{pmatrix} = \begin{pmatrix} S & P \\ T & P \\ O & A \end{pmatrix}$$

6. Solution

Using the Playfair matrix given below, encrypt the message: "Must see you over Cadogan West. Coming at once".

Plain text	mu	st	se	ey	ou	ov	er	ca	do	ga	nw	es	tc	om	in	ga	to	nc	ex
Ciphertext	UZ	TB	DL	GZ	PN	NW	LG	TG	TU	ER	OV	LD	BD	UH	FP	ER	HW	QS	RZ