# 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

1. **Solution**

|  |  |
| --- | --- |
| 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 |

1. **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



Receiver



Thus, the ciphertext is 011 000 010

1. **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 OZ O R R

Ciphertext: F F F L B C V F X

Plaintext: G R O U N D H O G

1. **Solution**

**Encryption:**

Message = 



Then we do the encryption:



Thus the ciphertext is: **ITN NEP**

**Dectryption:**

thus Key-1 exist, and we calculate the Key-1:

1. **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 |