Johns Hopkins ■ CS600.424: Network Security ■ Spring 2011

Homework 1 – Assignment

Due Date – February 17 in class

Instructions: Please do not submit handwritten assignment.

1. Using the monoalphabetic cipher given below, (a) encode the message “This is an easy problem.” (b) Decode the message “rmij u uamu xyj.”

```
plaintext:  abcdefghijklmnopqrstuvwxyz
ciphertext: mnbvcxzasdfghjklpoiuytrewq
```

2. Consider the block cipher shown on slide 11 of lecture notes covered in class. Suppose that each block cipher S_i simply reverses the order of 8 input bits (so that for example, 11110000 becomes 00001111). Further suppose that the 64 bit scrambler dos not modify any bits (so that the output value of the mth bit is equal to the input value to the mth bit. (a) With n=3 and original 64-bit input equal to 10100000 repeated eight times, what is the value of the output? (b) Repeat part (a) but now change the last bit of the original 64 bit input a 0 to 1. (c) Repeat part (a) and (b) but now suppose that the 64 bit scrambler inverses the order of bits. (Hint for (c) use $(A^R B^R C^R)^R$ = CBA, where A, B, C are bit strings, and R means inverse).

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

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

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

5. Using the Hill cipher for n = 3, and the matrix K given below encrypt the message STO PPA and the decrypt to recover original plaintext. Show all the work.

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

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

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