Johns Hopkins ■ CS600.424: Network Security ■ Spring 2012

Homework 1 – Solutions

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
```

   Solution:

   The encoding of “This is an easy problem” is “uasi si my cmiw lokngch”.

   The decoding of “rmij'u uamu xyj” is “wasn't that fun”.

2. Consider the block cipher shown on slide 27 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 m^{th} bit is equal to the input value to the m^{th} 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).

   Solution:

   (a) The output is equal to 00000101 repeated eight times.

   (b) The output is equal to 00000101 repeated seven times + 10000101.

   (c) We have (ARBRCR)R = CBA, where A, B, C are strings, and R means inverse operation. Thus:

      1. For (a), the output is 10100000 repeated eight times;

      2. For (b), the output is 10100001 + 10100000 repeated seven times.

3. Consider the 3 – bit block cipher table as shown on slide 25 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?

   Solution:

   (a) 100100100 ==> 011011011

   (b) Trudy will know the three block plaintexts are the same.

   (c) c(i) = KS(m(i) XOR c(i-1))

   c(1) = KS(100 XOR 111) = KS (011) = 100

c(2) = KS(100 XOR 100) = KS (000) = 110

c(1) = KS(100 XOR 110) = KS (010) = 101

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

Solutions:

To encrypt the plaintext message MILLENNIUM using the key YTWOK, we first translate the message and the key into their numerical equivalents. The letters of the message and the letters of the key translate to

$$p_1 p_2 p_3 p_4 p_5 p_6 p_7 p_8 p_9 p_1 \overline{0} = 12, 8, 11, 11, 4, 13, 13, 8, 20, 12$$

and

$$k_1 k_2 k_3 k_4 k_5 = 24, 19, 22, 14, 10,$$

respectively. Applying the Vigenere cipher with the specified key, we find that the characters in the encrypted message are:

$$c_1 = p_1 + k_1 = 12 + 24 \equiv 10 (\mathrm{mod}\, 26)$$
$$c_2 = p_2 + k_2 = 8 + 19 \equiv 1 (\mathrm{mod}\, 26)$$
$$c_3 = p_3 + k_3 = 11 + 22 \equiv 7 (\mathrm{mod}\, 26)$$
$$c_4 = p_4 + k_4 = 11 + 14 \equiv 25 (\mathrm{mod}\, 26)$$
$$c_5 = p_5 + k_5 = 4 + 10 \equiv 14 (\mathrm{mod}\, 26)$$
$$c_6 = p_6 + k_1 = 13 + 24 \equiv 11 (\mathrm{mod}\, 26)$$
$$c_7 = p_7 + k_2 = 13 + 19 \equiv 6 (\mathrm{mod}\, 26)$$
$$c_8 = p_8 + k_3 = 8 + 22 \equiv 4 (\mathrm{mod}\, 26)$$
$$c_9 = p_9 + k_4 = 20 + 14 \equiv 8 (\mathrm{mod}\, 26)$$
$$c_{10} = p_{10} + k_5 = 12 + 10 \equiv 22 (\mathrm{mod}\, 26)$$

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

To decrypt the ciphertext message FFFLB CVFX encrypted using a Vigenere cipher with key ZORRO, we first translate the letters of the ciphertext message into their numerical equivalents to obtain $c_1c_2c_3c_4c_5c_6c_7c_8c_9$=5 5 5 11 1 2 21 5 23. The numerical equivalents of the letters in the key are $k_1k_2k_3k_4k_5$ = 25 14 17 17 14. To obtain the numerical equivalents of the plaintext letters , we proceed as follows:

$$p_1 = c_1 - k_1 = 5 - 25 \equiv 6 (\mathrm{mod}\, 26)$$
$$p_2 = c_2 - k_2 = 5 - 14 \equiv 17 (\mathrm{mod}\, 26)$$
$$p_3 = c_3 - k_3 = 5 - 17 \equiv 14 (\mathrm{mod}\, 26)$$
$$p_4 = c_4 - k_4 = 11 - 17 \equiv 20 (\mathrm{mod}\, 26)$$
$$p_5 = c_5 - k_5 = 1 - 14 \equiv 13 (\mathrm{mod}\, 26)$$
$$p_6 = c_6 - k_1 = 2 - 25 \equiv 3 (\mathrm{mod}\, 26)$$
$$p_7 = c_7 - k_2 = 21 - 14 \equiv 7 (\mathrm{mod}\, 26)$$
$$p_8 = c_8 - k_3 = 5 - 17 \equiv 14 (\mathrm{mod}\, 26)$$
$$p_9 = c_9 - k_4 = 23 - 17 \equiv 6 (\mathrm{mod}\, 26)$$

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

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

Solution: Because det(A) $\equiv$5(mod 26), we have (det A, 26)=1. To encrypt a plaintext block of length three, we use the relationship

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} \equiv A \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} (\mathrm{mod}\, 26)$$

To encrypt the message STO PPA, we first split the letters into Blocks of three letters. We have plaintext blocks

STO PPA

We translate these letters into their numerical equivalents:

18 19 14 15 15 0

We obtain the block of ciphertext in the following way:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} \equiv \begin{bmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 19 \\ 14 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 19 \\ 13 \end{bmatrix} (\mathrm{mod}\, 26)$$

Similarly, for PPA we obtain Cipher text as C_1=13, C_2=4, C_3=15. Translating this message into letters, we have as ciphertext = “ITN NEP” . The decrypting process for this ploygraphic cipher system takes a ciphertext block and obtains a plaintext block using the transformation.

$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \equiv \bar{A} \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} (\text{mod } 26), \textit{where } \bar{A} = \begin{bmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & 3 & 7 \end{bmatrix},$$ which is an inverse of matrix A mod 26.

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

Solutions: UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ