Sai Vineet Reddy Thatiparthi February 14, 2019

CS-302 Problem Set 1

Collaborators: *Aditya P. and TS Harikrishnan*

Problem 1-1

Trying all the possibilities on the ciphertext *EVIRE*, one can see that it translates to both, the River and the Arena, for different values of k. Antony does not know where to meet Caesar as his message can mean both the possibilites.

Problem 1-2

The affine function given to us is $9x + 2\ mod\ 26$. If one compares this function to the encryption function of any affine cipher, it can be deduced that $\alpha = 9$ and $\beta = 2$.

The ciphertext given to us is **UCR**, or if we were to represent this text using integers, we get 20 2 and 17.

Let's decrypt it one letter at a time.

Letter U(20) ⇒

$$\Rightarrow D_k(20) = 9^{-1}(20 - 2)mod26$$
$$\Rightarrow D_k(20) = 3(18)mod26$$
$$\Rightarrow D_k(20) = 54mod26$$
$$\Rightarrow D_k(20) = 2$$

2 is also used to represent the letter **C**.

The inverse of number 9 in the mod 26 world is 3. That is why we replace is with the inverse of 9 in the above solution.

Similarliy, if we were to decrypt letter C(2) and R(17), we would get A(0) and T(19). This means that **UCR** decrypts to **CAT**.

Problem 1-3

(a) Eve has found out two plaintext and ciphertext pairs. She also knows that the hill cipher machine that is being used requires a 2 x 2 matrix to encrypt and decrypt.

BA is being encrypted to HC and ZZ is being encrypted to GT.

Let's assume that the matrix, K, being used is $K = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The encryption function of a hill cipher is $E_k(m_i) = Km_i$. Let's try to encrypt BA using the matrix K. BA can be represented using integers as 1 and 0.

$$c_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) * \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$$
$$c_1 = \left(\begin{smallmatrix} (a*1+b*0) \\ (c*1+d*0) \end{smallmatrix}\right)$$
$$c_1 = \left(\begin{smallmatrix} (a) \\ (c) \end{smallmatrix}\right)$$

We know that BA has been encrypted to HC (7 and 2). This means that since $C_1 = \left(\begin{smallmatrix} (a) \\ (c) \end{smallmatrix}\right)$ and also $\left(\begin{smallmatrix} 7 \\ 2 \end{smallmatrix}\right)$, we can deduce that a = 7 and c = 2.

Similarly, using the new found values of a and c in the matrix $K = \left(\begin{smallmatrix} 7 & b \\ 2 & d \end{smallmatrix}\right)$. Using this new matrix to find out the remaining values of b and d, we get

$$c_2 = \left(\begin{smallmatrix} 7 & b \\ 2 & d \end{smallmatrix}\right) * \left(\begin{smallmatrix} 25 \\ 25 \end{smallmatrix}\right)$$
$$c_2 = \left(\begin{smallmatrix} (7*25+b*25) \\ (2*25+d*25) \end{smallmatrix}\right)$$
$$c_2 = \left(\begin{smallmatrix} (175+b*25) \\ (50+d*25) \end{smallmatrix}\right)$$

We know that C_2 is GT, or 6 and 19. Using the above equations, we can deduce that -

$$175 + 25b = 6 mod 26$$

The above equation is true when the one of the values of b is 13. So, we can say that $b = 13$. Similarly,

$$50 + 25d = 19 mod 26$$

The above equation is true when the one of the values of d is 5. So, we can say that $d = 5$. The final matrix is $K = \left(\begin{smallmatrix} 7 & 13 \\ 2 & 5 \end{smallmatrix}\right)$

(b) For the cipher to work properly, one should be able to encrypt and decrypt. In a hill cipher, any cipher can be used to encyrpt, decryption is only possible if the inverse of the same matrix exists. This is because, the decryption function is $D_k(c) = K^{-1}m$.

If $K = \left(\begin{smallmatrix} 7 & 2 \\ 1 & 4 \end{smallmatrix}\right)$ is to be used for encryption, we need to see if the inverse of this matrix exists which allows decryption. The inverse of K would be

$$M^{-1} = \frac{1}{ad - bc} * \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$$

$$K^{-1} = \frac{1}{24} * \left(\begin{smallmatrix} 4 & -2 \\ -1 & 7 \end{smallmatrix}\right)$$

The matrix K can be used for encryption as it is invertible.

Problem 1-4

(a) We are given the following information -

Message probabilities

m	P(m)
5	1/3
6	1/3
7	1/6
8	1/12
9	1/12

We are also told that the same three keys, namely $0, 1, 2$, are to be used. The probability of choosing a key is the same at $1/3$. The distribution of probability across the keys and the messages (joint probability distribution) will be as shown in Table 1.

Let's assume that the system that Alice is currently using is perfectly secure. In any perfectly secure system, the ciphertext does not give out any information about the message. Formally put, this means that $P[m] = P[m|c]$.

	0	**1**	**2**
5	1/9	1/9	1/9
6	1/9	1/9	1/9
7	1/18	1/18	1/18
8	1/36	1/36	1/36
9	1/36	1/36	1/36

Table 1: Probability distribution

Let's try to put this equation to test. Alice wants to send a message m = 7. This gets encrypted to ciphertext c = 7.

$$P[m = 7] = \frac{1}{3}$$
$$P[m = 7|c = 9] = ?$$

We need to see if these two equations are the same. From table 1, the points where the resultant encrypted text is 9 will be when (following the format of message, key) (7,2), (8,1) and (9,0). The $P[c = 9]$ will be the sum of all the individual probabilities

$$P[c = 9] = \frac{1}{18} + \frac{1}{36} + \frac{1}{36}$$
$$P[c = 9] = \frac{1}{9}$$

The probability of the message being m = 7 and c = 9 can be looked from table 1 - $P[m = 7 \ \ \& \ \ c = 9] = \frac{1}{18}$.

So, the probability of

$$P[m = 7|c = 9] = \frac{P[m = 7 \ \ \& \ \ c = 9]}{P[c = 9]}$$
$$P[m = 7|c = 9] = \frac{\frac{1}{18}}{\frac{1}{9}}$$
$$P[m = 7|c = 9] = \frac{1}{2}$$

But if the system was perfectly secure, $P[m = 7|c = 9] = P[m = 7]$. But it does not seem to be the case. Hence, Alice's modified system is not perfectly secure.

(b) No, it is not possible to create new a system, despite the change in message probabilities, that is perfectly secure. This is because, the system being perfectly secure does not depend on the message probabilities at all, but rather the key and the message space. It is not possible to modify it without changing they message and key space.

(c) It is not possible to modify the existing system to make it perfectly secure, even after changing the message probabilities. However, if we make the message and the key space the same, while retaining the Caesar cipher becomes a perfectly secure system. The larger conclusion that one can draw from this exercise is that a system's ability to be perfectly secure does not depend on the message's probability rather the message and the key space instead.

Problem 1-5

(a) Shift Cipher In a shift cipher, all the letters in the cipher text are shifted by a predefined key k. Since the message being transmitted is the letter a repeated several times, the encrypted text will also be some letter (depending on k) repeated the same number of times. This allows Zark, who has intercepted the messages, to figure out that the message being sent is the same letter repeated multiple times.

However, because the letter is repeated multiple times and the cipher text is also some letter repeated multiple times, Zark cannot deduce which letter is being sent multiple times nor can he deduce the key as each letter is just as likely as the next.

(b) Affine Cipher In an Affine Cipher, after one chooses α and β, you can notice that each letter gets encrypted as the same letter each time. This means that, since the message being transmitted is the same letter repeated several times, the encrypted message will also have some letter repeated several times. Zark will figure out that the letter being sent is the same letter repeated multiple times. But he can not figure out what this letter is nor can he figure out the the key used to encrypt as each letter is as likely as the next.

(c) Hill Cipher (2 x 2) In a 2 x 2 hill cipher, 2 letters are encrypted at once by multiplying their integer equivalents with the matrix. Since the message being sent is the letter a repeated several, the number 00 will be multiplied with the matrix, which equals to 00 as well. This means that, even the encrypted text will be the same letter as the message being sent. Since Zuck knows what system is being used, he can figure out what the message is and also that it is repeating multiple times.

However, Zuck cannot figure out the 2 x 2 matrix key being used as the letter a will always result into being encrypted as 0, which is possible with any key.

Problem 1-6

I wrote a code to run brute force attacks on the given shift cipher texts.

(a) uryczrvzgenccrqvafvqrnpnrfnepvcurenaqpnagtrgbhg

HELP ME IM TRAPPED INSIDE A CAESAR CIPHER AND CANT GET OUT

(b) pfldljksvjgvvufwczxyksvtrljvkzdvjkfgjnyvezcffbrkpflyrggpmrcve kzevjurp

YOU MUST BE SPEED OF LIGHT BECAUSE TIME STOPS WHEN I LOOK AT YOU HAPPY VALENTINES DAY

(c) hgnodxnthmsdqbdossghrrdbqdssqzmrlhrrhnmvhsgntszmxdqqnqsghrsqz mrlhrrhnmgzrsqzudkkdczlhkkhnmkhfgsxdzqrsnhmenqlxntsgzsvdzqdbn lhmfrnnm

I HOPE YOU INTERCEPT THIS SECRET TRANSMISSION WITHOUT ANY ERROR THIS TRANSMISSION HAS TRAVELLED A MILLION LIGHT YEARS TO INFORM YOU THAT WE ARE COMING SOON

(d) khzzaxwuwjeowckkzkjaatyalpbkniahkjiahkjiahkjiahkjiahkj

OLD DEBAYAN IS A GOOD ONE EXCEPT FOR MELON MELON MELON MELON MELON

Problem 1-7

The code is attached along with the submission. One just needs to edit the *ciphertext* variable with the text before running it.

(a) Key: deaf

(b) Key: caesar

(c) Key: noes