**QUIZ CMPE-553 30.11.2020 (110 min, 16.30-18.20, 2 points)**

**Accepting of the Quiz paper will be closed at 18.35**

St. **Name, Surname**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Instructor Alexander Chefranov**

**Please, consider the instructions below.**

1. The Quiz1 assignment will become available on 30.11.2020, 16.30
2. Your answers shall be hand-written
3. On each page, at the top, write a header: “CMPE553 Quiz1 30.11.2020”, followed by your Name, Surname, Student ID, page number
4. There are **5** questions in total. Try answering each question. There are 2 pages in total.
5. You may rewrite the text of the question in your paper, or not. It is up to you. But at the beginning of an answer, write “Question <i> answer:” substituting <i> by a particular question number
6. Open book, open notes, work yourself
7. Copies are not allowed and will be zero graded
8. In **15 minutes after the exam finishing**, you shall do **all** the following. 1. Make photo of each your page so that its full content, including the header, is in the image, and clearly readable. 2. Then, the images shall be assembled in the page number order into a pdf file named “CMPE553 Quiz1 30112020 Name Surname.pdf”. 3. **Finally,** Upload the pdf file with answers; In the **case of uploading problems**, e-mail to Alexander.chefranov@emu.edu.tr
9. ***papers uploaded (sent) outside of the 15 minutes Stated in item 7 will not be considered for checking!!!***
10. ***Only one pdf file uploaded will be considered for checking!!!***

Good Luck!

**Task 1. (0.4 points)** Use Playfair cipher to encrypt “The weather” using key sentence “is good in November”. Show details of your work (how you fill the matrix, how you preprocess the plaintext, and how you get the ciphertext).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| i/j | s | g | o | d |
| n | v | e | m | b |
| r | a | c | f | h |
| k | l | p | q | t |
| u | w | x | y | z |

 Alphabet: 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

Present as pairs:

“the weather”=>th ew ea th er => TH=>ZT; EW=>VX; EA=>VC; TH=>ZT; ER=>NC

The ciphertext is: ZTVXVCZTNC

**Hint:**

Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that *balloon* will be treated as *ba lx lo on*
2. Plaintext letters that would fall in the same row of matrix are each replaced with the letter to the right, with the first element of the row circularly following the last.
3. Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last.
4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

**Task 2. (0.4 points)** Use Hill cipher to encrypt and decrypt back the plaintext “PLAIN” for English alphabet if the key matrix is

|  |  |
| --- | --- |
| 1 | 2 |
| 4 | 3 |

Give necessary explanations.

**Hint:** A-1[i,j]=(-1)i+jDji/det(A)

detA=3-8=-5 mod 26=21

(detA)-1 mod 26=5; Check: 21\*5=105 mod 26= 1

Extended Euclid algorithm to find the inverse:

1. A=(1,0,26), B=(0,1,21)

Q=floor(A3/B3)=floor(26/21)=1

T=A-Q\*B=(1,-1,5)

1. A=(0,1,21), B=(1,-1,5)

Q=floor(A3/B3)=floor(21/5)=4

T=A-Q\*B=(-4,5,1)

Since T3=1, and new B3=T3, the inverse is T2= new B2=5

D11=3; D12=4; D21=2; D22=1

A-1(1,1)=D11\*5 mod 26=3\*5 mod 26=15

A-1(1,2)=-D21\*5 mod 26=-2\*5 mod 26=-10 mod 26=16

A-1(2,1)=-D12\*5 mod 26=-4\*5 mod 26=-20 mod 26 =6

A-1(2,2)=D22\*5 mod 26=1\*5 mod 26=5

$$A^{-1}mod 26=\left(\begin{matrix}15&16\\6&5\end{matrix}\right)$$

Check correctness of the inverse

$$A∙A^{-1}mod 26=\left(\begin{matrix}1&2\\4&3\end{matrix}\right)\left(\begin{matrix}15&16\\6&5\end{matrix}\right)=\left(\begin{matrix}15+12&16+10\\60+18&64+15\end{matrix}\right)mod 26=\left(\begin{matrix}1&0\\0&1\end{matrix}\right)$$

Encoding:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Plain =>(15, 11, 0, 8, 13)

Split plaintext in blocks of size 2: P1=(15,11), P2=(0,8), P3=(13,23), using x=23 as a filler in the last not full block, P3

$C1=A∙P1 mod 26= \left(\begin{matrix}1&2\\4&3\end{matrix}\right)\left(\begin{matrix}15\\11\end{matrix}\right) mod 26=\left(\begin{matrix}15+22\\60+33\end{matrix}\right) mod 26=\left(\begin{matrix}11\\15\end{matrix}\right)$=”LP”

$C2=A∙P2 mod 26= \left(\begin{matrix}1&2\\4&3\end{matrix}\right)\left(\begin{matrix}0\\8\end{matrix}\right) mod 26=\left(\begin{matrix}0+16\\0+24\end{matrix}\right) mod 26=\left(\begin{matrix}16\\24\end{matrix}\right)$=”QY”

$C3=A∙P3 mod 26= \left(\begin{matrix}1&2\\4&3\end{matrix}\right)\left(\begin{matrix}13\\23\end{matrix}\right) mod 26=\left(\begin{matrix}13+46\\52+69\end{matrix}\right) mod 26=\left(\begin{matrix}7\\17\end{matrix}\right)$=”HR”

Ciphertext is “LPQYHR”

Decryption:

$P1'=A^{-1}∙C1 mod 26= \left(\begin{matrix}15&16\\6&5\end{matrix}\right)\left(\begin{matrix}11\\15\end{matrix}\right) mod 26=\left(\begin{matrix}165+240\\66+75\end{matrix}\right) mod 26=\left(\begin{matrix}15\\11\end{matrix}\right)$=”PL”

$P2'=A^{-1}∙C2 mod 26= \left(\begin{matrix}15&16\\6&5\end{matrix}\right)\left(\begin{matrix}16\\24\end{matrix}\right) mod 26=\left(\begin{matrix}240+384\\96+120\end{matrix}\right) mod 26=\left(\begin{matrix}0\\8\end{matrix}\right)$=”AI”

$P3'=A^{-1}∙C3 mod 26= \left(\begin{matrix}15&16\\6&5\end{matrix}\right)\left(\begin{matrix}7\\17\end{matrix}\right) mod 26=\left(\begin{matrix}105+272\\42+85\end{matrix}\right) mod 26=\left(\begin{matrix}13\\23\end{matrix}\right)$=”NX”

Thus, the plaintext decrypted matches the original plaintext.

**Task 3. (0.4 points)** Apply permutation P=(3,4,2,6,8,1,5,7) to (a,b,c,d,e,f,g,h), find inverse of P, and check its correctness. Give necessary explanations.

P(a,b,c,d,e,f,g,h)=(c,d,b,f,h,a,e,g)

P-1 =(6,3,1,2,7,4,8,5)

Check that P(P-1)=I=(1,2,3,4,5,6,7,8)

Actually, P(6,3,1,2,7,4,8,5)=(1,2,3,4,5,6,7,8)

**Task 4. (0.4 points)** For a 64-bit vector V=0x31 35 74 a5 21 ff ed fe in hexadecimal, what is the result of the DES Inverse Initial permutation transformation given below:

|  |
| --- |
| IP-1 |
|  40 8 48 16 56 24 64 3239 7 47 15 55 23 63 3138 6 46 14 54 22 62 3037 5 45 13 53 21 61 2936 4 44 12 52 20 60 2835 3 43 11 51 19 59 27 34 2 42 10 50 18 58 2633 1 41 9 49 17 57 25  |
|
|
|
|
|
|
|

Give necessary explanations

The bit string is V=

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
|  | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
|  | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
|  | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
|  | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
|  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|  | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
|  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |

|  |
| --- |
| Result of transformation: |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |

IP-1 places bits from the specified by a number position into the position of the number, e.g., bit 39 with value 0 is placed into position 9.

**Task 5. (0.4 points)** For the Caesar cipher, encrypt “CMPE Quiz” with substitution table constructed using the following key sentence: “the following key sentence”. Give necessary explanations.

Fill the substitution matrix by the symbols from the key sentence without repetitions, and the rest, by not appeared yet letters in the alphabetic order

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| plain | 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 |
| cipher | t | h | e | f | o | l | w | i | n | g | k | y | s | c | a | b | d | j | m | p | q | r | u | v | x | z |

Ciphertext: ESBODQNZ