**QUIZ CMPE-553 15.04.2013 (90 min, 2 points)**

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

Instructor Alexander Chefranov

**Task 1. (0.4 points)** Calculate the relative frequency of the letter ‘e’ occurrence in the following text:

“Two principal m**e**thods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext: One approach is to encrypt multiple letters of the plaintext (Playfair Cipher, Hill Cipher), and the other is to use multiple cipher alphabets (Polyalphabetic Ciphers)”

Show your calculations and explain them.

We count total number, Tot, of letters in the text, and number of occurrences of ‘e’, N(‘e’), in the text, the frequency of ‘e’, RF(‘e’)=N(‘e’)/Tot

N(‘e’)=9+10+10+5=19+15=34,

Tot=(3+9+7+3+4+2+12+7+2+6+3+6+2)

+(5+3+9+2+3+9+8+2+3+10+3+8+2+2+7)+

(8+7+2+3+9+8+6+4+6+3+3+5+2+2+3)+

(8+6+9+14+7)=66+76+71+44=142+115+257

RF(‘e’)=34/257

**Task 2. (0.5 points)** Check that an inverse modulo 26 of the matrix

K=

|  |  |  |
| --- | --- | --- |
| 17 | 17 | 5 |
| 21 | 18 | 21 |
| 2 | 2 | 19 |

exists. If it exists, calculate its element (2,1) on the cross of row 2 and column 1. Show your calculations and explain them.

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

Det(A)=17\*18\*19+17\*21\*2+21\*2\*5-2\*18\*5-21\*17\*19-2\*21\*17=(17\*18\*19-21\*17\*19)+(17\*21\*2-2\*21\*17)+210-180=-3\*17\*19+30=-51\*19+30=-950-19+30=-939mod26=-3mod26=23

det(A)-1=17 because 23\*17=391mod26=1

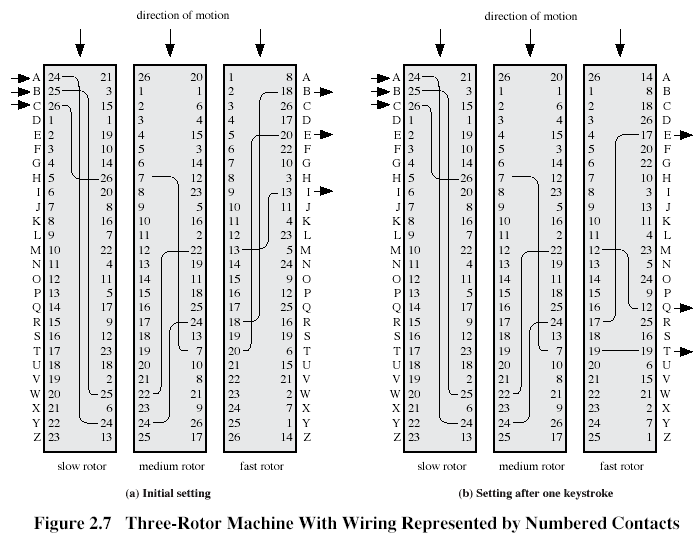
According to the hint, A-1[2,1]=(-1)2+1D12\*17=-17\*(21\*19-2\*21)=-17\*17\*21=-6069=-11mod26=15

**Task 3. (0.5 points)** Encipher the message “meet me after the toga party” with a rail fence of depth 3 (show the rail fence obtained by you and resulting ciphertext)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M |  | M |  | T |  | H |  | g |  | R |  |  |
|  | E | T | E | F | E | T | E | O | A | A | T |  |
|  |  | E |  | A |  | R |  | T |  | P |  | Y |

The ciphertext is mmthgretefeteoaateartpy

**Task 4. (0.5 points)** Consider the rotor machine below



What is the ciphertext for the plaintext ‘NO’?

N->11->14->7->X; O->12->18->15->V

The ciphertext is ‘XV’

**Task 5.**  **(0.4 points)** Determine what S-boxes in next round of DES algorithm are affected by the first output bit S-box S4 from the previous round. Explain your answer using information below:



|  |  |  |  |
| --- | --- | --- | --- |
| Expansion/Permutation (E table) | | | |
| 32 | 1 2 3 4 | 5 | |
| 4 | 5 6 7 8 | 9 | |
| 8 | 9 10 11 12 | 13 | |
| 12 | 13 14 15 16 | 17 | |
| 16 | 17 18 19 20 | 21 | |
| 20 | 21 22 23 24 | 25 | |
| 24 | 25 26 27 28 | 29 | |
| 28 | 29 30 31 32 | 1 | |
| Permutation function( P ) | | |
| 16 7 20 21 29 12 28 17  1 15 23 26 5 18 31 10  2 8 24 14 32 27 3 9  19 13 30 6 22 11 4 25 | | |

The 1st output bit of S4 is bit number 13 (see Fig. 3.9). Bit 13 is placed by the permutation P into position 26. Hence, this bit enters the next round in position 26. After Expansion/Permutation, bit 26 is used as a middle bit input for S7 only. Hence, the first output bit of S-box S4 in the previous round affects S-box S7 only in the next round.