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

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

Instructor Alexander Chefranov

**Task 1. (0.5 points)** Use Playfair cipher to encrypt “Encrypt this text” using key word “Mediterranean”. Show details of your work (how you fill the matrix, how you preprocess the plaintext, and how you get the ciphertext).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| m | e | d | i | T |
| r | a | n | b | C |
| f | g | h | k | l |
| o | p | q | s | U |
| v | w | x | y | Z |

En cr yp tx th is te xt

Da ra ws dz dl by md zd

**Task 2. (0.5 points)** Find inverse of the matrix below modulo 27 if it exists, or show that it does not exist.

K=

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

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

detK=17\*18\*19+21\*2\*5+~~17\*21\*2~~-2\*18\*5-21\*17\*19-~~2\*21\*17~~=17\*19\*(18-21)+(21-18)\*10=30-3\*17\*19=3\*(10-17\*19)=3\*(10-340+17)=-3\*313=-3\*(11\*27+16)mod27=-48mod27=-21mod27=6

As far as 6 and 27 are not relatively prime, gcd(6,27)=3<>1, inverse matrix does not exist

**Task 3. (0.5 points)** Consider



Encrypt “Encrypt” assuming initial state as shown on Fig. 2.7,a.

Encrypt

e-2-21-23-L, n-11-14-6-u, c-26-7-18-d, r-15-2-9-r, y-22-12-4-o, p-13-25-12-u, t-17-16-5-s

ludrous

**Task 4.**  **(0.5 points)** Determine what S-boxes in the next round of DES algorithm are affected by the first output bit S-box S3 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 28 171 15 23 26 5 18 31 102 8 24 14 32 27 3 919 13 30 6 22 11 4 25 |

The first output bit of S3 has number 9. Bit 9 after P will be in the position 24. Bit 24 of the output of the previous round will be used as input to S6, S7.