**MT Exam CMPE-553 18.04.20132 (90 min, 30 points)**

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

Instructor Alexander Chefranov

**Task 1. (7.5 points)** Consider S-DES encryption scheme below. Assume K1=’10101000’, input to the 1st round is ‘10110011’. What is the output of the 1st round of S-DES encryption? Provide intermediate results with explanations.



L0=1011 R0=0011

E/P(R0)=1001 0110+K1=0011 1110

S0(0011)=10 S1(1110)=00

P4(1000)=0001

L1=L0+0001=1010 R1=R0=0011

Take into account that

|  |
| --- |
| E/P |
| 4 1 2 3 2 3 4 1 |

 0 12 3 0 12 3



|  |
| --- |
| P4 |
| 2 4 3 1 |

**Task 2. (7.5 points)** Consider the rotor machine below



What is the ciphertext for the plaintext ‘THE’?

T=>17=>16=>11=>J; H=>5=>15=>4=>L; E=>2=>21=>21=>X

**Task 3. (7.5 points)** Prove that inverse of the matrix  mod 9 exists and find it. Check by example that found by you matrix is actually an inverse.

detK=8-6=2<>0 and gcd(2,9)=1 => K is invertible

(detK)-1=5: 2\*5=1mod9

K-1(1,1)=(-1) 1+1D11\*(detK)-1= 1\*8\*5=4mod9

K-1(1,2)=(-1) 1+2D21\*(detK)-1=-5\*2=8mod9

K-1(2,1)=(-1) 1+2D12\*(detK)-1=-5\*3=3mod9

K-1(2,2)=(-1) 2+2D22\*(detK)-1=5\*1=5mod9





**Task 4. (7.5 points)** Determine what S-boxes in the previous round of DES algorithm affect the 1st input bit of S-box S4 in the next 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 |

1st input of S4 is bit 12 of the right half R of the input to the next round.

Bit 12 of R is obtained in the previous round after permutation P of outputs of S-boxes and XOR-ing with L. Bit 12 after P is bit 26 after S-boxes. Bit 26 is output by S7. Hence, S7 from the previous round affects 1st input of S4 in the next round.