**MT Exam CMPE-553 5.12.2014 (90 min, 30 points)**

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

Instructor Alexander Chefranov

**Task 1. (7.5 points)** Use extended Vigenere cipher (26 English letters and 10 decimal digits) to encrypt “CMPE553” using key word “Mediterranean”. Show details of your work

Hint: Use modular arithmetic.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

CMPE553 is 2 12 15 4 31 31 29

Mediterranean is 12 4 3 8 19 4 17 17 0 13 4 0 13

Encrypt by adding modulo 36

C+M=2+12=14=o

M+e=12+4=16=q

P+d=15+3=18=s

E+i=4+8=12=m

5+t=31+19=50mod36=14=0

5+e=31+4=35=9

3+r=29+17=46mod36=10=k

Ciphertext is OQSMO9K

**Task 2. (7.5 points)** Find inverse of the matrix below modulo 27 and check its correctness by multiplication if it exists, or show that it does not exist.

A=

|  |  |
| --- | --- |
| 7 | 7 |
| 1 | 8 |

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

detA=7\*8-1\*7=56-7=49mod27=22; gcd(22,27)=1, hence detA-1 exists and equal to 16: 22\*16=382=13\*27+1

a-1[1,1]=8\*16=128mod27=20

a-1[1,2]=-7\*16=-112mod27=-4=23

a-1[2,1]=-1\*16=-16mod27=11

a-1[2,2]= 7\*16=112mod27=4

Check by multiplication



**Task 3. (7.5 points)** Consider



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

c-26-7-20-e

i-6-23-8-b

p-13-25-15-w

h-5-15-2-z

e-2-21-19-w

r-15-2-7-c

Ciphertext is EBWZWC

**Task 4.**  **(7.5 points)** Determine what S-boxes in the previous round of DES algorithm affect “middle” bits (bits 3 and 4) of the S-box S4 of 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 |

Middle bits of S4 are bits 14 and 15 coming from the previous round. Bit 14 is bit 18 output by S-box S5, and bit 15 is bit 31 output by S8. Hence, S5 and S8 in the previous round affect middle bits of S4 in the next round.