**MT Exam CMPE-553 08.12.2022 (90 min, 30 points)**

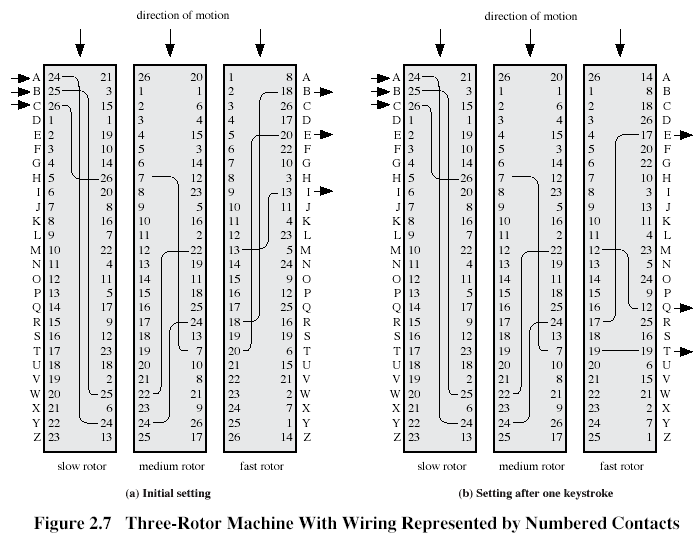
St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Mobiles and calculators are not allowed. Three cheat sheets with your own handwritings can be used**

Instructor Alexander Chefranov

**3 questions, 8 pages**

**Task 1. (10 points)** Encrypt the plaintext “te” by the Three-Rotor machine shown in Fig. 2.7 below. Assume the initial state as in Fig. 2.7, a. Explain you answer



Solution:

1. T=>slow rotor: 17=>17=>16 in medium rotor: 16=>16=>11 in fast rotor 11=>11=>J
2. State after 1 rotation of the fast rotor is shown in (b)

E=>2=>2=>21 in medium rotor 21=>21=>22 in fast rotor 22=>22=>G

Thus TE is encrypted as JG

**Task 2. (10 points)** Calculate the result of DES initial permutation, IP, transformation assuming that the plaintext block in hexadecimal is 0x12345678abcdef09. Show result in binary and hexadecimal. Explain you answer

HINT:

|  |
| --- |
| IP |
| 58 50 42 34 26 18 10 2  60 52 44 36 28 20 12 4  62 54 46 38 30 22 14 6  64 56 48 40 32 24 16 8  57 49 41 33 25 17 9 1  59 51 43 35 27 19 11 3  61 53 45 37 29 21 13 5  63 55 47 39 31 23 15 7 |

Solution

Plaintext in binary is

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 5 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 6 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 7 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 8 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

After permutation in binary

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

And in hexadecimal: 0x6c0f66f0705af855

**Task 3. (10 points)** Calculate {32}\*{34}+{56} in GF(2^8) with irreducible polynomial as in AES: . Show your intermediate calculations, and explain them.

Solution: {32}\*{34}=(0011 0010)\*(0011 0100)=(x^5+x^4+x)\*(x^5+x^4+x^2)=x^10+x^9+x^7+x^9+x^8+x^6+x^6+x^5+x^3= x^10+x^8+x^7+x^5+x^3. It is not in GF(2^8), hence, reduce it:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient |
| x^10+x^8+x^7+x^5+x^3  +  x^10+x^6+x^5+x^3+x^2= | x^8+x^4+x^3+x+1 | x^2+1 |
| x^8+x^7+x^6+x^2  +  x^8+x^4+x^3+x+1= |  |  |
| x^7+x^6+ x^4+x^3+x^2+x+1 remainder |  |  |

Thus, as it shall be

dividend=quotient\*divisor+ remainder

Check it:

quotient\*divisor+ remainder =( x^2+1)\*( x^8+x^4+x^3+x+1)+ x^7+x^6+ x^4+x^3+x^2+x+1=x^10+x^6+x^5+x^3+x^2+ x^8+x^4+x^3+x+1+ x^7+x^6+ x^4+x^3+x^2+x+1= x^10+x^5+ x^8+ x^7+x^3= x^10+x^8+x^7+x^5+x^3=dividend, OK

Thus, {32}\*{34}=(0011 0010)\*(0011 0100)=(x^5+x^4+x)\*(x^5+x^4+x^2)= x^7+x^6+ x^4+x^3+x^2+x+1=(1101 1111)={df}

{32}\*{34}+{56}={df}+{56}=

1101 1111

+

0101 0110=

1000 1001={89}