**Eastern Mediterranean University**

**Computer Engineering Department**

**CMSE-353 Security of Software Systems**

 **Midterm Exam**

**Three A4 sheets of paper with your handwritings may be used for your help. Photocopies, printouts, etc. are not allowed! Electronic devices are not allowed**

**Duration: 90 Minutes December 3, 2022**

**Std Id\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Std Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Instructor Alexander Chefranov**

**Totally 4 questions, 6 pages**

**Q1.** **(25 points).** What is Availability security requirement? Explain why it is important to secure systems

Availability requirement is as follows: a system shall be available to authorized users inside time periods agreed between the system and the clients. It is important to secure systems because if it is not available it the agreed time, it negatively affects business processes the system supports (e.g., telemedicine operation) and cause deaths, malfunction, blackouts, etc. Also, reputation of the system suffers.

**Q2. (25 points).** What is Mandatory access control model? What two rules does it use? Explain importance of each of the both rules for security of the systems

Mandatory access control model assigns security levels to subjects (users, processes) and objects (files, databases, etc.) as Unclassified, Confidential, Secret, and Top secret, associated with numbers 0,1,2, and 3, respectively. Read access of the subject with level i is allowed to object of level j if i>=j, known as “no read-up” rule. Write access of the subject with level i to the object of level j is allowed if i<=j, known as “no write-down” rule. “No read-up” rule is used to provide confidentiality: users of low levels as Unclassified, can’t read confidential, secret, or top secret documents. “No write-down” rule countering Trojan horse attack aiming leakage of secrets from top-level user to low-level users. This rule, as “no read-up” rule, provides confidentiality requirement.

Q3. (25 points). Given DES 64-bit master key in hexadecimal form as 0xabcdeffedcba0110, what is the result of Permuted choice 1 (PC-1) in binary and hexadecimal? Explain your answer.

# Hints:

#

|  |
| --- |
| Permuted Choice 1 (PC-1) |
| 57 49 41 33 25 17 91 58 50 42 34 26 1810 2 59 51 43 35 2719 11 3 60 52 44 36 |
| 63 55 47 39 31 23 157 62 54 46 38 30 2214 6 61 53 45 37 2921 13 5 28 20 12 4 |

**Secret key in binary:**

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

**Result of PC-1 in binary moving bits according to PC-1 as bit 57 goes to position 1, bit 49 goes to position 2, etc., bit 4 goes to position 56:**

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

 **Result of PC-1 in hexadecimal is**

**0x3f 1e 2d b2 d1 e3 f8**

**Q4.** **(25 points).** In GF(2^8) with irreducible polynomial m(x)=x^8+x^4+x^3+x+1 calculate {5a}\*{7b}. Show your calculations, give necessary explanations.

Hints:

**Mix Column Transformation**

The forward mix column transformation, called MixColumns, operates on each column individually. Each byte is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined as the following matrix multiplication on State (Fig. 5.5b):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |  | S00 | S01 | S02 | S03 |  | S00’ | S01’ | S02’ | S03’ |  |
| 01 | 02 | 03 | 01 | \* | S10 | S11 | S12 | S13 | = | S10’ | S11’ | S12’ | S13’ | (5.3) |
| 01 | 01 | 02 | 03 |  | S20 | S21 | S22 | S23 |  | S20’ | S21’ | S22’ | S23’ |  |
| 03 | 01 | 01 | 02 |  | S30 | S31 | S32 | S33 |  | S30’ | S31’ | S32’ | S33’ |  |

Each element in the product matrix is the sum of products of elements of one row and one column. In this case, multiplications and additions are performed in GF(28).

The following is the example of MixColumns;

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 87 | F2 | 4D | 97 |  | 47 | 40 | A3 | 4C |
| 6E | 4C | 90 | EC | => | 37 | D4 | 70 | 9F |
| 46 | E7 | 4A | C3 |  | 94 | E4 | 3A | 42 |
| A6 | 8C | D8 | 95 |  | ED | A5 | A6 | BC |

1st column of the result is obtained by:

{02){87}+{03}{6E}+{46}+{A6} = {47}

{87}+{02}{6E}+{03}{46}+{A6} = {37}

{87}+{6E}+{02}{46}+{03}{A6} = {94}

{03}{87}+{6E}+{46}+{02}{A6} = {ED}

For the 1st equation, we have {02}{87}=(0000 0010)(1000 0111)=

=

(0001 0101)={15}

{5a}\*{7b}=(0101 1010)\*(0111 1011) =(x^6+x^4+x^3+x)\*(x^6+x^5+x^4+x^3+x+1) = x^12+x^11+x^10+x^9+x^7+x^6+ x^10+x^9+x^8+x^7+x^5+x^4+ x^9+x^8+x^7+x^6+x^4+x^3+ x^7+x^6+x^5+x^4+x^2+x =

x^12+x^11+ x^9+x^6+x^4+x^3+x^2+x

Divide it by x^8+x^4+x^3+x+1:

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | quotient |
| x^12+x^11+ x^9+x^6+x^4+x^3+x^2+x+x^12+x^8+x^7+x^5+x^4= | x^8+x^4+x^3+x+1 | x^4+x^3+x+1 |
| x^11+x^9+x^8+x^7++x^6+x^5+x^3+x^2+x+x^11+x^7+x^6+x^4+x^3= |  |  |
| x^9+x^8+x^5+x^4+x^2+x+x^9+x^5+x^4+x^2+x= |  |  |
| x^8+x^8+x^4+x^3+x+1= |  |  |
| x^4+x^3+x+1 remainder |  |  |

Check correctness

Quotient\*divisor+remainder=dividend?

(x^4+x^3+x+1)\*( x^8+x^4+x^3+x+1)+ x^4+x^3+x+1=

x^12+x^8+x^7+x^5+x^4+ x^11+x^7+x^6+x^4+x^3+ x^9+x^5+x^4+x^2+x+ x^8+x^4+x^3+x+1+x^4+x^3+x+1= x^12+ x^11+ x^9+x^6+x^4+x^3+x^2+x = dividend

Thus, result is x^4+x^3+x+1=(0001 1011) = {1b}