**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 November 11, 2023, 8.30**

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

**Instructor Alexander Chefranov**

**Totally 4 questions, 6 pages**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Task** |  |  |  |  | **Total** |
| **Points** | **25** | **25** | **25** | **25** | **100** |

**Task 1.** **(25 points).**

1. (5 points) What a message authentication code (MAC) is?

MAC is a hash of the message concatenated with a secret key;

1. (5 points) What for is MAC used?

MAC is used for the message authentication

1. (5 points) How MAC is calculated by a sender?

MAC(M,K)=hash(M||K)

1. (5 points) What is sent by a sender to protect a message by MAC?

A sender sends a two-component packet: (M, MAC(M, K))

1. (5 points) How does a receiver verify the message authenticity protected by MAC?

On receipt of the packet (M’, MAC’), a receive verifies it by checking: hash(M’||K)==MAC’. If yes, it is authentic and accepted, otherwise, rejected.

**Task 2. (25 points).**

1. (5 points) What for passwords are used?

The passwords are used for users authenticaion

1. (5 points) Why passwords are considered as sensitive information?

Passwords are considered sensitive information because if becoming known to hackers they can be used for masquerading attack.

1. (15 points) Enlist five attacks on passwords
2. Dictionary attack
3. Stealing paper with a password written
4. Social security pretexting technique

4) Social security quid pro quo technique

5) Use of the spyware (keylogger)

**Task 3. (25 points).** Given DES 64-bit master key as an 8-character string “DeS kEy1”, what is the result of Permuted choice 1 (PC-1) in binary and hexadecimal? To answer, fill in blanks in the Answer section below. 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 |

 |
|  |  |

**Task 3 Answer Section**:

1. (5 points) Secret key in hexadecimal: DeS kEy1 = 0x44 65 53 20 6b 45 79 31\_
2. (7 points) Secret key in binary:

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

1. (8 points) Result of PC-1 in binary:

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

1. (5 points) Result of PC-1 in hexadecimal: 0x0077dac1423504\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 4. (25 points).** Given 128-bit AES plaintext block as a 16-character string P=“1234567890abcdef” and the 1st round key as also a 16-character string K1=“0123456789abcdef”, what is the value of the first two bytes of the transformed plaintext after AddRoundKey and SubstituteBytes transformations. Give your answers in the Answer Section below. Show your calculations, give necessary explanations.

Hints:

ASCII Table is given in the hints to Task 3.

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

**Task 4 Answer Section:**

1. (4 points) Plaintext in hexadecimal form as a 1D array

0x\_\_31323334353637383930616263646566\_\_\_\_\_\_

1. (4 points) Plaintext in hexadecimal form as a state array

|  |  |  |  |
| --- | --- | --- | --- |
| 0x\_31\_ | 0x\_35\_ | 0x\_39\_ | 0x\_63\_ |
| 0x\_32\_ | 0x\_36\_ | 0x\_30\_ | 0x\_64\_ |
| 0x\_33 | 0x\_37\_ | 0x\_61\_ | 0x\_65\_ |
| 0x\_34\_ | 0x\_38\_ | 0x\_62\_ | 0x\_66\_ |

1. (4 points) Round key K1 as a 1D array

0x\_30313233343536373839616263646566\_\_\_\_\_\_\_\_\_

1. (4 points) Round key K1 as a 4x4 matrix

|  |  |  |  |
| --- | --- | --- | --- |
| 0x\_30\_ | 0x\_34\_ | 0x\_38\_ | 0x\_63\_ |
| 0x\_31\_ | 0x\_35\_ | 0x\_39\_ | 0x\_64\_ |
| 0x\_32\_ | 0x\_36\_ | 0x\_61\_ | 0x\_65\_ |
| 0x\_33\_ | 0x\_37\_ | 0x\_62\_ | 0x\_66\_ |

1. (5 points) The first two bytes calculated:

1st byte: 0x31+0x30=0x01\_\_\_\_=>7c\_\_\_\_\_\_\_\_\_\_\_\_

2nd byte: 0x31+0x32=0x03\_\_\_\_=>7b\_\_\_\_\_\_\_\_\_\_\_\_

1. (4 points) The first two bytes calculated in the proper places of the output state array

|  |  |  |  |
| --- | --- | --- | --- |
| 0x\_7c\_ | 0x\_\_ | 0x\_\_ | 0x\_\_ |
| 0x\_7b\_ | 0x\_\_ | 0x\_\_ | 0x\_\_ |
| 0x\_\_ | 0x\_\_ | 0x\_\_ | 0x\_\_ |
| 0x\_\_ | 0x\_\_ | 0x\_\_ | 0x\_\_ |