|  |  |  |
| --- | --- | --- |
| Course: | **Information Security** | Date: 08/04/2023 |
| Course Code: | CSC – 407 | Session: II |
| Faculty’s Name: | Dr. Hafiz Ishfaq Ahmed & Ms. Nighat Usman | Max Marks: 30 |
| Time Allowed: | 1.5 Hours | Total Pages: (12) |

**Solution**

**Question # 1 (2\*3 Marks)**

Answer the followings in your own wordings.

1. Differentiate Symmetric encryption scheme and asymmetric encryption scheme.
2. Describe about the cryptanalysis and also explain at the end that how brute force attack works? Discuss the cryptanalytic attacks.
3. Discuss the concept behind Rotor machines.

...................................…………………..………………………….………………………………..…… (CLO-2)

**Question # 2 (4\*2 Marks)**

1. For the following keywords and given ciphertext, perform the Playfair Cipher.

Keyword: BACKGROUND

Cipher Text: QLSYSYUDELRISELZMEVMWCQV

Plain Text: ??

1. Apply Vigenere Cipher Decryption method on the given ciphertext and discover the plaintext.

Ciphertext = abqdvmwuwjphfvvyyrfznydokvl

Keyword = HUMOR

...................................…………………..………………………….………………………………..…… (CLO-1)

**Question # 3 (4 Marks)**

Consider a general enciphering scheme where streaming bits are given,

Plaintext = 1011 0101 110

Ciphertext is 0001 0110 111

Compute the secret key, for the given Plaintext and Ciphertext.

...................................…………………..………………………….………………………………..…… (CLO-1)

**Question # 4 (4\*3 Marks)**

1. Explain the working of DES in form of bullets and draw diagram as well.
2. While working with DES, you have received

C9 = 0101010101111111100001100110

D9 = 0011110001111010101010110011

Generate C10, D10 and K10 by solving the example for Round 10.

1. If S-Boxes return the following bits:

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 0101 1100 1000 0010 1011 0101 1001 0111

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

Now, perform the remaining steps to get R1 (right) value.

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

...................................…………………..………………………….………………………………..…… (CLO-4)