Master of Computer Application

MCAC302: Information Security

Semester III
Year of Admission: 2021

Time: 1 Hour **Max. Marks: 15**

Note:
1. Attempt all parts of a question together.
2. Use of calculators is not allowed.

1. (a) If all messages are of the same length and a message is never repeated, then is it secure to re-use the same one-time pad for encryption? Justify your answer. (3)

   (b) Encipher the following message using the Hill Cipher with key = "*FILM*". (2)
   "*INCEPTION*"

   ~~2x1~~ ~~4x1~~

2. Rank the following substitution ciphers in the order of the magnitude of confusion they create. Justify your answer. (3)
   (a) Vernam Cipher
   (b) Monoalphabetic Cipher
   (c) Ceaser Cipher

3 (a) Alice and Bob agree to use *Playfair* cipher for the secret communication with Key = *SECRET*, *x* as the special character used for padding and i and j are treated as the same character. For a particular message, Bob receives the cipher text C= *ITCSITEUOHAMCZ*. Provide a detailed description of the decryption process followed by Bob. (3)

   (b) Find the multiplicative inverse of 26187 modulo 1533 using the Extended Euclidean algorithm. (1)

4 Why is the worst-case time complexity of executing a "*Known Plaintext*" attack on a 112-bit key *Double DES* is $O(2^{56})$ and not $O(2^{112})$? Explain. (3)

156
78 78
78
56
22

156
112
44

56

56

FI INCEP
LM TIONX

2x5

2x2 2x5
2x5

~~4x1~~ ~~4x~~
1x4 4x3
1x3

Scanned with CamScanner