



Inter-State School Of Higher Education
PAUL BIYA TECHNOLOGICAL CENTRE OF EXCELLENCE
P.O Box 13 719 Yaoundé (Cameroon) Tel. (237) 22 72 99 58
Web site: www.iaicameroun.com E-mail: iaicameroun@yahoo.fr

Test of Cryptography

Level: II Academic year: 2020/2021 Branch: Software Engineering Duration: 02h

Structural (10MKS)

1. Differentiate between Cryptography and STEGANOGRAPHY and state one example in each case.....2MKS
2. Who is a cryptanalyst?.....1Mks
3. Differentiate between with examples.....2MKS
 - i. Polyalphabetic and Monoalphabetic techniques in Cryptography.....2Mks
 - ii. Block Cipher and Stream Cipher.....2Mks
 - iii. ECB, CBC and CFM.....3MKS
4. $L=4, m=4, k\text{-round}=3-3-2-1-5-6, N=5, K=1010011010111011, X=1010001110110111$

Using SPN encrypt the above plaintext X. 5MKS

MCQ Section (Right = .5 Wrong = -.25) 5 MKS

1. The _____ is the original text.
A) ciphertext B) plaintext C) secret-text D) none of the above
2. The _____ is the message after transformation
A) ciphertext B) plaintext C) secret-text D) none of the above
3. Message _____ means that the data must arrive at the receiver exactly as sent.
A) confidentiality B) integrity C) authentication D) none of the above
4. The _____ cipher reorders the plaintext characters to create a ciphertext.
A) Substitution B) transposition C) steganography technique D) None of the above
5. One commonly used public-key asymmetric cryptography method is the _____ algorithm.
A) DES B) ECB C) RSA D) CBC
6. A(n) _____ algorithm transforms cipher text to plaintext.
A) Encryption B) Decryption C) Either (a) or (b) D) Neither (a) nor (b)
7. A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.
A) S-box B) P-box C) T-box D) none of the above
8. A _____ cipher replaces one character with another character of the same text.
A) Substitution B) Transposition C) Either (a) or (b) D) Neither (a) nor (b)
9. A combination of an encryption algorithm and a decryption algorithm is called a _____.
A) Cipher B) secret C) key D) none of the above
10. In an asymmetric-key cipher, the sender uses the _____ key to encrypt his message.
A) private B) public C) external D) neither (a), (b) nor (b)

GOOD LUCK☺