Princess Sumaya University for Technology
The King Hussein School for Information Technology
Second Semester 2016/2017
Information System Security

A

Second Exam **Wedneday: 13/11/2016**

SID:…….. **Name:**……..

Hint: using the following alphabitcal order: a b c d e f g h i j k l m n o p q r s t u v w x y z

Topic: Classical Encryption Technique
Question (1) (7 Points)

a) brute force attack is try all keys to get plaintext from ciphertext. Based on the brute force attack how many keys you are try if using Monoalphabetic Cipher technqiue. **(1 Point)**
Answer:

b) Encrypthe the "**Hello**" **by using playfair** cipher, if the key is "**Playfair**". **(2 Points)**
Answer:

c) If the Key read is: 2 5 4 1 3, what is the key Write? **(1 Point)**
Answer

d) Decrypt the "**YGHCTAPRYROP**" by using **Columnar Transposition Ciphers**, if the key is "**3412**". **(1.5 Points)**

e) Decrypt the "**anerassinoe**" by using **Fixed Transposition Ciphers**, if the key is "**2413**". **(1.5 Points)**
Answer:

Topic: Modern Encryption Technique (S-DES, DES, 3DES)
Question (2) (5.5 Points)

a) The mathematical form for S-DES is

$$\textbf{Ciphertext} = IP^{-1}(F_{K2}(SW(F_{K1}(IP(\text{Plaintext})))))$$

Assume developed new vesrion from S-DES called PSUT-DES that have three stage. Based on that, write the mathematical form for the decryption in the PSUT-DES algorithm. **(1.5 Points)**
Answer:

b) **In S-DES Assume the key (K) is 10111 00010**
Calculate the first key K1, K2 for Key (K= 10111 00010). **(2 Points)**

c) Assume the following is the input for **DES s-boxes**
100000 001000 100000 010000 000000 001101 000000 000110
What is the output from **DES S-boxes for S1 and S3**? Write the results in hexdecimal. **(2 Points)**

Question (3) (4.5 Points)

a) Show the first eight words of the key expansion for a **128-bit key of all zeros in AES**. **(3 points)**
Answer:

b) **In AES** Given the plaintext {00010203040506070809 0A0B0C0D0E0F} and the key {01010101010101010101010101010101} **(1.5 Points)**
Show the original contents of **State**, displayed as a 4×4 matrix
Answer:

Question 4: (8 Points)

a) **(RSA)** In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M? **(3 Points)**

b) **Write the answer of the following (5 Points)**

1. -38 mod 15 =
2. 73 ≡ ..... mod 23
3. If a ≡ b mod n, then (a – b) mod n
4. If a ≡ b mod n, then b ≡
5. 11^7 mod 13 =
6. GCD(8,15) =
7. Is 6 and 35 are relatively prime? And why?
8. Determine φ(*7*).
9. Determine φ(*6*).
10. Determine all Primitive root for 7.