Uva Wellassa University, Sri Lanka
Faculty of Science and Technology
2nd Semester Examination September/October 2012

CST 342-2 Cryptographic Systems

Uva Wellassa University

Time Duration : Two Hours (2 hrs.)
Number of Pages : Three (3)
Answer All Questions

Part A: Short Answer Questions (21 x 2 = 42 marks)

Write your answers clearly. Keep your answers neat and very brief.
Messy or long answers will not be marked.

1. Differentiate Private Key and Public Key.
2. What do you mean by Authentication Protocols?
3. What is a Salted Password?
4. What is an Asymmetric Key?
5. What is a Dictionary Attack?
6. What are the drawbacks of Restricted Algorithms?
7. Differentiate Stream Ciphers and Block Ciphers.
8. What is Man-In-the-Middle Attack?
9. What is SKEY Algorithm?
10. Clarify Wide-Mouth-Frog Protocol.
11. What are the general types of operations used for transforming Plaintext to Ciphertext?
12. What is Brute Force Attack?
13. Differentiate Ceasor Cipher and ROT13.
14. Describe the access control types used in Firewalls.
15. What are the three types of Firewall Configurations?
16. Distinguish between Virus and Worms.
17. What is a Trojan Horse?
18. State five states of Warm(one of Malwares) Technologies.
19. Give two types of Virus Counter Measurements.
20. Distinguish between Link Encryption and End-To-End Encryption.
21. What is Front End Processor Function in Transport Layer Protocol?

PART B - (6 x 3 = 18 marks)

1. What does the following message say?

   JRQH WR ZDWFK KDUOHTXLQV.EDFN DW VHYHQ.

   Hint: Note that you can shift by any amount (Ex: 2,3,4.....).

2. Use "wellassa" as the key for Simple Columnar Transposition Cipher and find out the Plaintext for Ciphertext given below.

   orter emsns sxhao ifmer spapc tihil lairl xunoi yxtnp cai

3. Decode the following message using Caesar Cipher with shift + 5

   ltytufwnx

4. Use Rail Fence Technique with depth = 2 to decipher the below message.

   Welcome to the Uva Wellassa University

5. Consider a=22, X_0=1, c=0 and m=72 as the values of the equation of Linear Congruential Generator and construct the random number sequence up to 10 digits. You should choose the correct equation for the Linear Congruential Generator from the equations given below.

   i. $X_n = (aX_{n-1}+c) \bmod m$
   ii. $X_n = (aX_{n+1}+c) \bmod m$
   iii. $X_{n+1} = (aX_n+c) \bmod m$
   iv. $X_{n+1} = (cX_n+a) \bmod m$

6. Let p=11, q=19 and s=3 and calculate the Blum-Blum-Shub random number sequence up to 6 digits[$X_0 = s^2 \bmod (p \times q)$].
   You should select the correct equation for the BBS among following equations.

   i. $X_{i+1} = X_i \bmod p$
   ii. $X_{i+1} = X_i^2 \bmod q$
   iii. $X_{i+1} = X_i \bmod p*q$
   iv. $X_{i+1} = X_i^2 \bmod p*q$

PART C – Long Answer Questions (20 x 2 - 40 marks)

Make your answers as clear and easy to understand as possible. Provide diagrams and brief comments where necessary. Confusing, difficult to understand or illegible answers will lose marks.

1.

a. Draw a neat flow chart to describe the steps in RSA Algorithm. **(6 marks)**

b. Discuss about the efficiency of RSA. **(4 marks)**

c. Suppose that the Alice send a message "12" to the Bob using RSA Algorithm. She has selected two prime numbers 31 and 23 for "p" and "q" respectively and 223 as the values of "e". Perform the Encryption and Decryption on this message using RSA Algorithm. **(10 marks)**

2.

a. Discuss in detail Data Encryption Standard Algorithm. **(12 marks)**

b. Explain about the Avalanche Effect. **(4 marks)**

c. What are the strengths of Data Encryption Standard Algorithm? **(4 marks)**

51