Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 2nd Semester Examination – Dec./Jan. 2017
CST342-2 Cryptographic Systems

Uva Wellassa University

Instructions to candidates:
Duration: 02 hours
Number of questions: Four (04)
Answer all questions
Mark allocation: 100
Calculators are allowed.

1.

a. Define the term Cryptanalysis. (3 mark)

b. List four (04) applications of Digital Certificates. (4 mark)

c.

i. What is meant by a Public Key Infrastructure (PKI)? (3 mark)

ii. What are the key elements of a typical PKI? (5 mark)

iii. What are the issues encountered with PKI? (5 mark)

d. Explain the involvement of a Key Distribution Center (KDC) in order to reduce the risks inherent in exchanging keys related to symmetric encryption. (5 mark)

2.

a.

i. Decrypt the following ciphertext with Caesar Cipher (shift key = 3). The decryption function is specified as:
$e(x) = (x - k) \ (mod\ 26)$
Where k is the key (the shift) applied to each letter.
Ciphertext: **ghswrifvw**
(5 mark)

ii. Using appropriate examples, explain different types of operations used for transforming plaintext to ciphertext, including substitution and transposition. (5 mark)

b. Encrypt the following plaintext with Rail-fence Cipher (Key = 4)
Plaintext: **uvawellassauniversityofsrilanka**
(5 mark)

c. Explain the encryption principle used in Jefferson Wheel Ciper. (5 mark)

d. Identify two (02) major improvements found in modern encryption algorithms compared to ancient encryption techniques. (5 mark)

51

3.

a.

i. Explain why, increase of computing power and discovery of more efficient factoring algorithms are concerned as the challenges to the RSA encryption algorithm.
(5 mark)

ii. Critically analyze the strength of DSA crypto-algorithm in the perspective of the key generation strategy.
(5 mark)

b.

i. Briefly explain the technique used in Data Encryption Standard (DES) encryption algorithm to reduce a 48 bit encrypted (XORed with a 48 bit subkey) half-data block in to a 32 bit output.
(5 mark)

ii. Encode the bit string 1101 0101 with the key 0010 1011.
(Hint: Use XOR Addition)
(2 mark)

c. i. What are the improvements done for the DES in order to derive Triple DES (3DES)?
(4 mark)

ii. During the AES encryption, each round (except the last round) consist of four (04) processing phases. What is/are the operation(s) not being performed (excluded) on the last iteration of AES encryption?
(4 mark)

4.

a.

i. What is cryptographic hash function? (2 mark)

ii. Briefly explain the functionality of typical cryptographic hash function.
(4 mark)

iii. List three (03) possible techniques those can be used for cracking a hash function.
(3 mark)

b.

i. Discuss the security aspects of the Enigma encryption machine in the context of secret communication occurred during the World War II.
(4 mark)

ii. What is meant by Password Authentication Protocol (PAP)? (2 mark)

iii. Explain the term Evil Twin (a form of Session hijacking) with an appropriate graphical illustration.
(5 mark)

c.

i. What is SQL injection? (2 mark)

ii. What are the commonly used intrusion detection techniques for mobile wireless networks?
(3 mark)