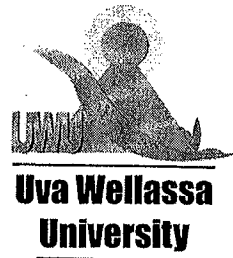


Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
End Semester Examination September/October 2013
CST 342-2 Cryptographic Systems



Instructions to Candidates

Time Duration : Two Hours (02 hrs.)

Number of Questions : Four (04)

Answer **All** Questions.

You are **not allowed** to use any external materials in the examination.

1. "The security of encryption scheme must depend only on the secrecy of the key and not on the secrecy of the algorithms" - Kirchhoff's Principle.
 - a. Justify above statement with at least three reasons. (3 mark)
 - b. Write **Shanon** characteristics for a good encryption algorithm. (5 mark)
 - c. Explain why a good cryptographic encryption algorithm will necessarily have a large key size. (5 mark)
 - d. Explain two party authentication and third party authentication. (4 mark)
 - e. Bob has RSA public key ($e=11, n=143$) and RSA private key ($d=11, n=143$). Alice has RSA public key ($e=23, n=170$) and RSA private key ($d=7, n=170$). Assuming the role of Alice and showing all steps clearly, **encrypt** and **decrypt** the message $M=40$ to be sent to Bob.
(It is not required to simplify the final answer) (8 mark)
2.
 - a. Determine the greatest common divisor of 1500 and 560. (4 mark)
 - b. Describe the SQL injection attack through a Web application by using an example. (5 mark)
 - c. In certain situations, a user has to revoke his digital certificate. What are the reasons for such revocations? (5 mark)

- d. Write **five** types of digital payment systems. What are the three domains involved in 3D secure? (8 mark)
- e. Personal Identification Numbers (PIN) used with ATM cards to draw money out of a cash machine has only four/six decimal digits. Why is it safe to have PINs of only four/six digits even though we would normally recommend that passwords be longer than this? (3 mark)
- 3.
- a. What are computer viruses? Explain the four phases of a computer virus. (6 mark)
- b. Define the term "Logic Bomb", and distinguish it from a computer virus. (4 mark)
- c. Generic Decryption and Digital Immune System are two advanced antivirus techniques, state all steps involved in a Digital Immune System. (6 mark)
- d. What is intrusion detection and explain two main intrusion detection approaches with its categories. (6 mark)
- e. Write three reasons for design a Honeypot in cryptographic systems. (3 mark)
- 4.
- a. What is a firewall? Write three characteristics of a good firewall. (5 mark)
- b. Define following terms and explain the relationship between them
- i. Security Policies
 - ii. Security Associations
 - iii. Security Policies Database (SPD)
 - iv. Security Associations Database (SAD)
- (6 mark)
- c. A wireless network has several vulnerabilities. State three such vulnerabilities. (3 mark)
- d. List all steps of a SSL handshake protocol. (5 mark)
- e. What are the required attributes used to identify a user or an issuer according to the X.509 standard? (6 mark)