ITS335 – Quiz 3

Name: _____ ID: _____ Marks: _____ (10)

Question 1 [3 marks]

There are 4 users in a public-key cryptosystem: *Preecha*, *Peeranont*, *Kamolchanok* and *Vasana*. Assume all relevant keys, e.g. (PU_{Meerit},PR_{Meerit}), have been generated and distributed. The public key encryption/decryption algorithms are denoted as E(key,message) and D(key,message), a hash algorithm is H(message) and concatenation is ||.

(a) Preecha has a message M to send to Kamolchanok. Write an equation that shows what is sent across the network to ensure the message will be confidential. [1.5 marks]

(b) Peeranont has a message M to send to Vasana. Write an equation that shows what is sent across the network to ensure the receiver will be able to authenticate the message (confidentiality is not required). [1.5 marks]

Question 2 [3 marks]

(a) The process of converting a coded message back to the original message is called _____.

(b) _____ is a security service that assures data received are exactly as sent.

(c) In a _____ attack, a malicious user pretends to be someone they are not.

Question 3 [2 marks]

Explain the difference between the three common malicious software propagation methods: worm, virus and social engineering.

Question 4 [2 marks]

Select all of the true statements from the list below by selecting the letter (a), (b), (c) or (d). Zero (0) or more statements may be true. [penalty for incorrect or missing selections]

(a) A countermeasure is a way to deal with an attack

(b) In the context of computer security objectives, CIA is refers to Central Intelligence Agency

(c) Symmetric key cryptography is used to provide confidentiality; it cannot provide authentication

(d) RSA is public key cipher that is considered secure

Question 5 [2 marks]

You have the task of implementing a login system. Explain an advantage and disadvantage of the following mechanism with respect to password usage. Be specific about the advantage (e.g. what attacker it can prevent) and disadvantage (e.g. what is a problem if used).

Generate random passwords for users.

Question 6 [2 marks]

A symmetric key cipher uses a 48-bit key. An attacker has obtained a ciphertext and is attempting a brute-force attack to find the key. The attacker plans to purchase computers so that in the worst case they can find the key within 2^{24} seconds. If each computer can decrypt at a speed of 2^{16} per second, how many computers are needed? Show your calculations.