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) Peeranont 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) Preecha 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) In a ________________________ attack, a malicious user changes the contents of an intercepted message.

(b) The process of converting an original message into a coded, apparently random message is called ________________________.

(c) ________________________ is a security service that assures a system is always accessible to authorised users.

Question 3 [2 marks]

Explain the difference between a normal virus, a metamorphic virus and a polymorphic virus, including discussing how easy they are to detect by anti-virus software.

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

(b) It is normally assumed the attacker knows the ciphers (algorithms)

(c) AES is public key cipher that is considered secure

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

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).

Require users to change their password every month.

Question 6 [2 marks]

A symmetric key cipher uses a 50-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.