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 Preecha. Write an equation that shows what is sent across the network to ensure the message will be confidential. [1.5 marks]

(b) Vasana has a message M to send to Kamolchanok. 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) ____________________ is a security service that assures the received data originated from the claimed sender.

(b) In a ____________________ attack, a malicious user sends an identical copy of a previous message they have intercepted.

(c) The information known only to sender and receiver in a cipher is called a____________________

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) AES is symmetric block cipher that is considered secure

(b) All block ciphers use a 64-bit key

(c) In the context of computer security objectives, CIA is refers to Confidentiality, Integrity and Authentication

(d) RSA is symmetric block 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).

Restrict the number of failed login attempts per day.

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^{23} seconds. If each computer can decrypt at a speed of 2^{16} per second, how many computers are needed? Show your calculations.