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) Vasana has a message M to send to Peeranont. 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 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 controls who can have access to a resource.

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

(c) In a ____________________ attack, a malicious user observes patterns of communications, without having to read the message contents.

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) In the context of computer security objectives, CIA is refers to Confidentiality, Insurance and Attackers

(b) Threats are potential violations of security policy that exploit vulnerabilities

(c) Triple DES (3DES) is more secure than DES, but is slower

(d) In computer security, assets consist of vulnerabilities, threats and attacks

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 have passwords that contain a mixture of uppercase, lowercase, digits and punctuation characters.

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^{15} per second, how many computers are needed? Show your calculations.