Answered by: Marcus Domingo

CS 468, Assignment 1

THEORY/WRITTEN QUESTIONS (100 points)

1) Multiple Choice [30 points]

I. A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is _____ .

A) integrity B) encryption

C) analysis D) masquerade

II. _____ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

A) Disruption B) Replay

C) Denial of Service D) Masquerade

III. Techniques used for deciphering a message without any knowledge of the enciphering details is _____ .

A) blind deciphering B) steganography

C) cryptanalysis D) transposition

IV. _____ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

A) Brute-force B) Cryptanalytic

C) Block cipher D) Transposition

V. The _____ attack is the easiest to defend against because the opponent has the least amount of information to work with.

Answered by: Marcus Domingo

A) ciphertext-only B) chosen ciphertext

C) known plaintext D) chosen plaintext

VI. _____ is the most common method used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

A) Symmetric encryption B) Data integrity algorithms

C) Asymmetric encryption D) Authentication protocols

2) Short Answers [70 points]

I. What are the practical problems that we face when using a symmetric key encryption system? What can the attacker focus on to defeat the cryptographic system beyond just bruteforce attacks?

In a system where two or more people are involved the key must be shared among them, making it less secure. The key should be changed frequently for each communication session. The attacker could focus on intercepting the key instead of the brute-force attack approach.

II. What is the one-time pad? How is it being used? Are there any practical limitations?

The one-time pad uses a one-time random secret key that is the same size or larger than the plaintext to be encrypted. They are being used in the more secret circumstances where the secrecy of the message outweighs the limitations of the encryption model. One well-known example is with nuclear launch messages as in the movie *Crimson Tide*. The limitations include that a new key has to be produced with every message and the size of the key has to be at least the same size as well as shared with sender and receiver.

III. When is steganography useful? Can it be equated to encryption?

Answered by: Marcus Domingo

Steganography is useful when more than two parties are involved in the sending and receiving of the message, such as tweets on Twitter. It can't be equated to encryption because with encryption you know you have a message to crack, but with steganography you must determine if the message has an underlying message first then try and decipher it, otherwise the message could go undetected.

IV. Can we use both steganography and encryption at the same time? If yes how can we apply both? Justify your answer.

Yes, you can create your steganography message then encrypt it or you can create your encrypted message and hide that in a steganography message. Both ways would prolong decrypting the message.

V. How can we know when the code implementation of a cryptographic algorithm is correct to use? Justify your answer.

We can check to see if the algorithm is FIPS 140-2 certified, which is a government standard for computer security that is used to approve cryptographic algorithms.

VI. Can code optimizations affect the cryptographic strength of encryption algorithms? Justify your answer.

No, code optimization allows the program to run efficiently and should not affect the strength of the algorithm.

VII. If we perform a double encryption using the same symmetric algorithm twice, do we double the key size space and thus the security of the DES algorithm? (Example: Double DES has a 112-bit key and enciphers blocks of 64 bits). Justify your answer.

No, you undo the encryption of the DES algorithm. Since the algorithm is symmetric it means the same key and the same steps are used to encrypt and decrypt, so therefore if you ran your plaintext through the same algorithm twice you would end up with the same plaintext.