Name: _____

ITCS 412: Cryptography

Student Number: _____

Exam 1,First semester 2006/2007, Form: A

Section: _____

Section 1.

	S1	Q1	Q2	Q3	Q4	Q5	Total
Maximum	13	5	5	5	5	5	38
Grade							

Answer the following questions by clearly circling *the most appropriate* answer. (1 points each)

1. The main problem with the security of the DES algorithm was
   (a) the length of the key.
   (b) the subkey generation method.
   (c) the block size.
   (d) the S-boxes.
2. Both Shannon and Berkhoff suggested the security through obscurity doesn't work well. Thus they suggested that security should only depend on knowledge of
   (a) the algorithm
   (b) the key
   (c) the plaintext
   (d) all of the above
3. What is the main component in a Feistel network that is responsible for diffusion?
   (a) the subkeys.
   (b) the swap operation.
   (c) the S-box.
   (d) the initial permutation (IP).
4. Which of the following is a security service, as defined in the X.800 standard?
   (a) Data origin authentication.
   (b) Modification of message.
   (c) Repudiation.
   (d) Digital signature.
5. Which of the following software can be used for sniffing and protection of the network from attacks?
   (a) nmap.
   (b) a keylogger.
   (c) snort.
   (d) superscan.

6. The only non-linear part of the DES input manipulation is done in
   (a) the S-boxes.
   (b) the initial permutation.
   (c) the XOR.
   (d) the swap.
7. Prevents either the sender or receiver from denying a transmitted message
   (a) Integrity.
   (b) Vulnerability.
   (c) Nonrepudiation.
   (d) Traffic analysis.
8. Port scanning is considered as
   (a) a passive attack.
   (b) part of footprinting.
   (c) a known plaintext attack.
   (d) a ciphertext only attack.
9. Statistical analyis of the frequency of the letters was an effective attack for breaking
   (a) monoalphabetic ciphers.
   (b) the Vigenere cipher.
   (c) both (a) and (b).
   (d) none of the above.
10. Which of the following factors makes the design and security of a block cipher worse?
   (a) Increasing the complexity of the encryption algorithm.
   (b) Increasing the number of rounds.
   (c) Increasing the key size.
   (d) Increasing the block size.
11. Which of the following is a pervasive security mechanism according to the X.800 standard?
   (a) Encipherment.
   (b) Security recovery.
   (c) Notarization.
   (d) Access control.
12. Most security mechanisms depend on a single technology for their implementation, which of the following is it?
   (a) integrity.
   (b) access.
   (c) identification.
   (d) encryption.

13. Which of the following is harder to attack using brute force?
    (a) DES.
    (b) Polyalphabetic cipher with 10-character (in ASCII) key.
    (c) Playfair cipher.
    (d) Caesar's cipher.

Section 2. Answer all of the following questions(5 points each)

1. Write the formula for a two stage Feistel network, and show that decryption is the inverse of encryption.

2. List three known attacks on DES. (Just list the name of each attack.)

3. Note that a basic rule of cryptography is that encryption is reversible. This allows decryption to be done. Consider what happens in the S-boxes of DES. The input is to the S-Box is 48 bits, but the output is only 32. Does this mean that the data is lost? Answer with yes or no.

   Explain your answer briefly.

4. Describe two possible countermeasures to keylogging.

   Describe two solutions to stop sniffing attacks.

5. Consider the one-time pad cipher.

   (a) List the three conditions for a one-time pad to be a perfectly secure cipher.

   (b) Describe briefly why it is considered impractical.

Answer Key for Exam A

Section 1.

	S1	Q1	Q2	Q3	Q4	Q5	Total
Maximum	13	5	5	5	5	5	38
Grade							

Answer the following questions by clearly circling *the most appropriate* answer. (1 points each)

1. The main problem with the security of the DES algorithm was
   - [(a)] the length of the key.
   - (b) the subkey generation method.
   - (c) the block size.
   - (d) the S-boxes.
2. Both Shannon and Berkhoff suggested the security through obscurity doesn't work well. Thus they suggested that security should only depend on knowledge of
   - (a) the algorithm
   - [(b)] the key
   - (c) the plaintext
   - (d) all of the above
3. What is the main component in a Feistel network that is responsible for diffusion?
   - [(a)] the subkeys.
   - (b) the swap operation.
   - (c) the S-box.
   - (d) the initial permutation (IP).
4. Which of the following is a security service, as defined in the X.800 standard?
   - [(a)] Data origin authentication.
   - (b) Modification of message.
   - (c) Repudiation.
   - (d) Digital signature.
5. Which of the following software can be used for sniffing and protection of the network from attacks?
   - (a) nmap.
   - (b) a keylogger.
   - [(c)] snort.
   - (d) superscan.
6. The only non-linear part of the DES input manipulation is done in
   - [(a)] the S-boxes.
   - (b) the initial permutation.
   - (c) the XOR.
   - (d) the swap.

7. Prevents either the sender or receiver from denying a transmitted message
   (a) Integrity.
   (b) Vulnerability.
   (c) Nonrepudiation.
   (d) Traffic analysis.

8. Port scanning is considered as
   (a) a passive attack.
   (b) part of footprinting.
   (c) a known plaintext attack.
   (d) a ciphertext only attack.

9. Statistical analyis of the frequency of the letters was an effective attack for breaking
   (a) monoalphabetic ciphers.
   (b) the Vigenere cipher.
   (c) both (a) and (b).
   (d) none of the above.

10. Which of the following factors makes the design and security of a block cipher worse?
   (a) Increasing the complexity of the encryption algorithm.
   (b) Increasing the number of rounds.
   (c) Increasing the key size.
   (d) Increasing the block size.

11. Which of the following is a pervasive security mechanism according to the X.800 standard?
   (a) Encipherment.
   (b) Security recovery.
   (c) Notarization.
   (d) Access control.

12. Most security mechanisms depend on a single technology for their implementation, which of the following is it?
   (a) integrity.
   (b) access.
   (c) identification.
   (d) encryption.

13. Which of the following is harder to attack using brute force?
   (a) DES.
   (b) Polyalphabetic cipher with 10-character (in ASCII) key.
   (c) Playfair cipher.
   (d) Caeser's cipher.

Section 2. Answer all of the following questions(5 points each)

1. Write the formula for a two stage Feistel network, and show that decryption is the inverse of encryption.

2. List three known attacks on DES. (Just list the name of each attack.)

3. Note that a basic rule of cryptography is that encryption is reversible. This allows decryption to be done. Consider what happens in the S-boxes of DES. The input is to the S-Box is 48 bits, but the output is only 32. Does this mean that the data is lost? Answer with yes or no.

   Explain your answer briefly.

4. Describe two possible countermeasures to keylogging.

Describe two solutions to stop sniffing attacks.

5. Consider the one-time pad cipher.

   (a) List the three conditions for a one-time pad to be a perfectly secure cipher.

   (b) Describe briefly why it is considered impractical.