Name: _____

CSC 371: Cryptography

Student Number: _____

Exam 1, Second semester 2003/2004, Form: A

Section: _____

Section 1.

For each question below choose the most appropriate answer and circle clearly only one choice of the following questions (3 points each).

1. Which of the following is a necessary property of a cipher to be more secure?
   (a) Analyzing the algorithm is more complex.
   (b) Running time of decryption must be large.
   (c) Ease of analysis of the algorithm.
   (d) Must be a one way function.
2. In a Feistel network, which of the following will prevent the decryption from being the reverse of the encryption
   (a) if the function F is not reversable
   (b) if the swap is not done in the rounds
   (c) key is not long enough
   (d) None of the above.
3. Which of the following ciphers does both confusion and diffusion:
   (a) DES.
   (b) Vigenere.
   (c) Caeser's.
   (d) Playfair.
4. Confusion in modern block ciphers is usually done by
   (a) The initial permutation and the switch.
   (b) The S-boxes.
   (c) The key generation.
   (d) None of the above.
5. What is the key for the following cipher text message "P VDDS RPI XC IWT WPI"?
   (a) a.
   (b) f.
   (c) n.
   (d) p.
6. The subkeys in DES are
   (a) 64 bit long.
   (b) 56 bit long.
   (c) 48 bit long.
   (d) 32 bit long.

7. For brute force attacks to be useful we must
   (a) have a distributed machine.
   (b) know the structure or language of the plaintext.
   (c) have a plaintext-ciphertext pair.
   (d) all of the above.
8. Which of the following will not increase the security of a modern block cipher?
   (a) Increase the complexity of the subkey generation.
   (b) Increasing the block size.
   (c) Use a linear function F.
   (d) None of the above.

Section 2. (5 points each)

1. Define the meaning of an *unconditionally secure cipher* and give one example for such a cipher.

2. Describe briefly two advantages and two disadvantages of cipher block chaining mode (CBC).

3. Use the Playfair cipher to encrypt the message *dont eat at macdonalds* using the key word CLEAR.

4. Specify three problems with the one-time pad cipher which make it impractical.

5. Consider what happens inside the function F of the DES cipher. The bits of the right half enter an expansion permutation, and the output is also permuted before entering the XOR. Are these permutations considered as part of the diffusion process which Shannon said is necessary to build strong ciphers? Explain your answer.

6. List three problems with DES which make it too weak as a secure cipher in the 21st century.

List two techniques which can be used to stop attackers from using timing attacks on DES.

Answer Key for Exam A

Section 1.

For each question below choose the most appropriate answer and circle clearly only one choice of the following questions (3 points each).

1. Which of the following is a necessary property of a cipher to be more secure?
   (a) Analyzing the algorithm is more complex.
   (b) Running time of decryption must be large.
   (c) Ease of analysis of the algorithm.
   (d) Must be a one way function.

2. In a Feistel network, which of the following will prevent the decryption from being the reverse of the encryption
   (a) if the function F is not reversable
   (b) if the swap is not done in the rounds
   (c) key is not long enough
   (d) None of the above.

3. Which of the following ciphers does both confusion and diffusion:
   (a) DES.
   (b) Vigenere.
   (c) Caeser's.
   (d) Playfair.

4. Confusion in modern block ciphers is usually done by
   (a) The initial permutation and the switch.
   (b) The S-boxes.
   (c) The key generation.
   (d) None of the above.

5. What is the key for the following cipher text message "P VDDS RPI XC IWT WPI"?
   (a) a.
   (b) f.
   (c) n.
   (d) p.

6. The subkeys in DES are
   (a) 64 bit long.
   (b) 56 bit long.
   (c) 48 bit long.
   (d) 32 bit long.

7. For brute force attacks to be useful we must
   (a) have a distributed machine.
   [(b)] know the structure or language of the plaintext.
   (c) have a plaintext-ciphertext pair.
   (d) all of the above.
8. Which of the following will not increase the security of a modern block cipher?
   (a) Increase the complexity of the subkey generation.
   (b) Increasing the block size.
   [(c)] Use a linear function F.
   (d) None of the above.

Section 2. (5 points each)

1. Define the meaning of an *unconditionally secure cipher* and give one example for such a cipher.

2. Describe briefly two advantages and two disadvantages of cipher block chaining mode (CBC).

3. Use the Playfair cipher to encrypt the message *dont eat at macdonalds* using the key word CLEAR.

4. Specify three problems with the one-time pad cipher which make it impractical.

5. Consider what happens inside the function F of the DES cipher. The bits of the right half enter an expansion permutation, and the output is also permuted before entering the XOR. Are these permutations considered as part of the diffusion process which Shannon said is necessary to build strong ciphers? Explain your answer.

6. List three problems with DES which make it too weak as a secure cipher in the 21st century.

List two techniques which can be used to stop attackers from using timing attacks on DES.