ITCS 412: Cryptography

Name: _____

Midterm 1, Second Semester 2008/2009

Student ID: _____

Section: _____

This exam consists of 4 pages.
Duration: 50 minutes

	Section 1	Section 2	Total
Maximum	21	19	40
Grade			

Section 1:

Answer the following questions by clearly circling *the most appropriate* answer. (1.5 points each)

1. Which of the following is considered a passive attack
   a. Release of message content
   b. Traffic analysis
   c. Replay and monitoring.
   d. Denial of service

2. Which of the following is considered an Access Control service
   a. File and Folder sharing
   b. Printer sharing
   c. Control Panel Access
   d. All of the Above

3. Which of the following is considered a Denial of service attack
   a. massive amount of ping traffic (ICMP echos) is sent to the broadcast address of the network
   b. Attacks take advantage of opened network services on the target (ports) and send massive amount of UDP echo data to network broadcast addresses
   c. Sending packets to the target with oversized payloads.
   d. All of the above

4. How to prevent a Denial of service attack
   a. making the routers not forwarding broadcast directed traffic to the network
   b. Installing patches and updates
   c. Installing firewall with filters.
   d. All of the above.

5. What are the basic two functions used in encryption algorithms?
   a. Permutation and substitution
   b. XOR and S-Boxes
   c. XOR and Sub-key generation
   d. XOR and Swap

6. What are the two general approaches to attacking a cipher?
   a. Cryptanalysis and brute force
   b. Frequency distribution and guessing
   c. Chosen plaintext chosen cipher text
   d. Frequency distribution and known plaintext

7. Known plaintext attack on encrypted messages requires knowledge of
   a. Encryption algorithm and ciphertext.
   b. Encryption algorithm, ciphertext, chosen ciphertext by cryptanalysis with its corresponding plaintext.
   c. Encryption algorithm, ciphertext, and one or more plaintext-ciphertext pairs.
   d. Encryption algorithm, ciphertext, and plaintext chosen by cryptanalysis with its corresponding ciphertext.

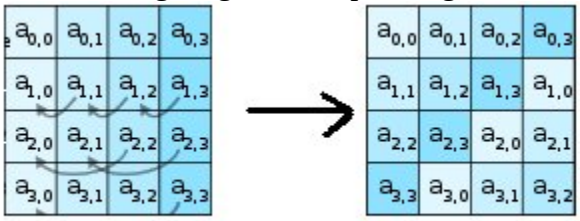
8. Steganography is
   a. Hiding the existence of a message
   b. Transposition of message letters
   c. Hiding the key used for encrypting the message
   d. Permutation of message letters

9. The Avalanche effect,
   a. Small change in key or plaintext produces a significant change in ciphertext
   b. Introduces non-linearity in key and ciphertext.
   c. Adds transformation complexity when XORed with substitution function, hence ciphertext
   d. All of Above

10. What is the purpose of the state matrix in AES,
   a. Hide plaintext structure
   b. Hide key transformation
   c. Hold substitution information
   d. Hold intermediate results

11. Using brute force attack, how many keys on average are searched to break a cipher with key size of 24-bits.
   a. 2^{23}
   b. 2^{24}
   c. 2^{12}
   d. Non of the above

12. The following diagram is expressing one of AES operations,



a. SubBytes Step
b. ShiftRows Step
c. MixColumns Step
d. AddRound Key Step

13. Consider the following form of ciphering a plaintext *p*

$$C = (a.p + b) \bmod 26$$

where *a* and *b* are some integers. A basic requirement of any encryption algorithm is that it be one-to-one (i.e. NO more than one plaintext character maps into the same ciphertext character) otherwise decryption is impossible. Which of the following values are allowed for *a* and *b*:

a. a=3 , b=4
b. a=4, b=3
c. a=13, b=3
d. a=2, b=3

14. Assume that you have a chip that includes four DES units working in parallel. Each DES unit takes one clock cycle to complete one encryption. How many clock cycles are needed using one of these chips to encrypt a 512-bit message?

a. 1
b. 2
c. 4
d. 8

Section 2:

Answer all of the following questions

1. Name one Advantage and one limitation of Cipher Block Chaining (CBC)? (4 points)

2. Write the formula for a two stage Fiestel encryption. (4 points)

3. Briefly describe MixColumns in AES and the rational behind adopting it. (4 points)

4. Arrange the following ciphers according to the size of their key space (largest to smallest): (3 points)

Double DES
One time pad
Caesar
AES w/256

5. A Vigenere cipher with key “ABCDE” has been used to encode a certain message, and the result is

D Q Q K W B V

Decode this string to find the original message. (Assume the alphabet is A, B, C .., Y, Z, space). Show your work. (4 points)

ITCS 412: Cryptography

KEY ANSWER

This exam consists of 4 pages.
Duration: 50 minutes

	Section 1	Section 2	Total
Maximum	21	19	40
Grade			

Section 1:

Answer the following questions by clearly circling *the most appropriate* answer. (1.5 points each)

1. Which of the following is considered a passive attack
   e. Release of message content
   f. Traffic analysis
   g. Replay and monitoring.
   h. Denial of service

2. Which of the following is considered an Access Control service
   e. File and Folder sharing
   f. Printer sharing
   g. Control Panel Access
   h. All of the Above

3. Which of the following is considered a Denial of service attack
   e. massive amount of ping traffic (ICMP echos) is sent to the broadcast address of the network
   f. Attacks take advantage of opened network services on the target (ports) and send massive amount of UDP echo data to network broadcast addresses
   g. Sending packets to the target with oversized payloads.
   h. All of the above

4. How to prevent a Denial of service attack
   e. making the routers not forwarding broadcast directed traffic to the network
   f. Installing patches and updates
   g. Installing firewall with filters.
   h. All of the above.

5. What are the basic two functions used in encryption algorithms?

e. Permutation and substitution
f. XOR and S-Boxes
g. XOR and Sub-key generation
h. XOR and Swap

6. What are the two general approaches to attacking a cipher?
e. Cryptanalysis and brute force
f. Frequency distribution and guessing
g. Chosen plaintext chosen cipher text
h. Frequency distribution and known plaintext

7. Known plaintext attack on encrypted messages requires knowledge of
e. Encryption algorithm and ciphertext.
f. Encryption algorithm, ciphertext, chosen ciphertext by cryptanalysis with its corresponding plaintext.
g. Encryption algorithm, ciphertext, and one or more plaintext-ciphertext pairs.
h. Encryption algorithm, ciphertext, and plaintext chosen by cryptanalysis with its corresponding ciphertext.

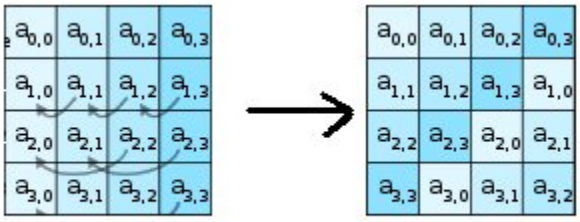
8. Steganography is
e. Hiding the existence of a message
f. Transposition of message letters
g. Hiding the key used for encrypting the message
h. Permutation of message letters

9. The Avalanche effect,
e. Small change in key or plaintext produces a significant change in ciphertext
f. Introduces non-linearity in key and ciphertext.
g. Adds transformation complexity when XORed with substitution function, hence ciphertext
h. All of Above

10. What is the purpose of the state matrix in AES,
e. Hide plaintext structure
f. Hide key transformation
g. Hold substitution information
h. Hold intermediate results

11. Using brute force attack, how many keys on average are searched to break a cipher with key size of 24-bits.
e. 2^{23}
f. 2^{24}
g. 2^{12}
h. Non of the above

12. The following diagram is expressing one of AES operations,



e. SubBytes Step
f. ShiftRows Step
g. MixColumns Step
h. AddRound Key Step

13. Consider the following form of ciphering a plaintext *p*

$$C = (a.p + b) \bmod 26$$

where *a* and *b* are some integers. A basic requirement of any encryption algorithm is that it be one-to-one (i.e. NO more than one plaintext character maps into the same ciphertext character) otherwise decryption is impossible. Which of the following values are allowed for *a* and *b*:

e. a=3 , b=4
f. a=4, b=3
g. a=13, b=3
h. a=2, b=3

14. Assume that you have a chip that includes four DES units working in parallel. Each DES unit takes one clock cycle to complete one encryption. How many clock cycles are needed using one of these chips to encrypt a 512-bit message?

e. 1
f. 2
g. 4
h. 8

Section 2:

Answer all of the following questions

1. Name one Advantage and one limitation of Cipher Block Chaining (CBC)? (4 points)

Advantage: uses bulk data encryption authentication.
Each ciphertext block depends on all message blocks
A change in message affects all cipher text blocks.

Limitation: requires an intial value IV
Decryption can not be performed in parallel.

2. Write the formula for a two stage Fiestel encryption. (4 points)

S) L1 = R0
R1 = L0 xor F(R0, K)

L2 = R1
R2 = L1 xor F(R1, K)

3. Briefly describe MixColumns in AES and the rational behind adopting it. (4 points)

Sol) MixColumns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. This gives good mixing of the bytes within each column provides good avalanche.

4. Arrange the following ciphers according to the size of their key space (largest to smallest): (3 points)

Double DES
One time pad
Caesar
AES w/256

5. Q) A Vigenere cipher with key "ABCDE" has been used to encode a certain message, and the result is

D Q Q K W B V

Decode this string to find the original message. (Assume the alphabet is A, B, C .., Y, Z, space). Show your work. (4 points)

S) Congrat