ITCS 412: Cryptography

Final Exam, First semester 2005/2006, Form: A

Name: _____

Student Number: _____

Section: _____

Section 1.

Circle the most suitable answer for the following questions/statements. (2 points each)

1. The attacker tries every possible key. What is the name of this attack?
   (a) Chosen plaintext.
   (b) Known plaintext.
   (c) Chosen key.
   (d) Brute force.
2. Which of the following algorithms works better when attacking the RSA algorithm?
   (a) Euclid's algorithm.
   (b) General number field sieve.
   (c) Special number field sieve.
   (d) Quadratic sieve.
3. All of the following are strong points of the PGP application except
   (a) It's available worldwide including its source code.
   (b) It includes many strong ciphers like DES, AES, Blowfish, IDEA, and CASE-128.
   (c) It provides a key distribution authority for the public keys.
   (d) It is not controlled by government agencies.
4. Decoy systems that are used to lure potential attackers are called
   (a) Intrusion Luring Systems.
   (b) Markov models.
   (c) Expert systems.
   (d) Honeypots.
5. Which of the following is the most useful and promising password selection strategy?
   (a) Proactive password checking.
   (b) Reactive password checking.
   (c) Computer generated passwords.
   (d) User education.
6. Which of the following is not a polyalphabetic cipher?
   (a) one-time pad.
   (b) Caeser's cipher.
   (c) Vigenere's cipher.
   (d) DES.

7. The design of DES is now considered as vulnerable to attacks because of
   (a) The number of rounds.
   (b) The block size.
   (c) It's too slow.
   (d) The key size.
8. Which of the following modes is useful for high-speed requirements and is provably as secure as the others?
   (a) ECB.
   (b) CBC.
   (c) OFB.
   (d) CTR.
9. Which of the following is not considered as a parameter in the design of a Feistel network?
   (a) Subkey generation algorithm.
   (b) Round function.
   (c) The exclusive-OR function.
   (d) Block size
10. The permutations done inside the S-box are considered by Shannon as part of the
   (a) confusion.
   (b) diffusion.
   (c) both (a) and (b)
   (d) neither (a) nor (b).
11. The simplest measure in statistical anomaly detection is
   (a) Multivatriate measure.
   (b) Markov process.
   (c) Time series analysis.
   (d) Mean and standard deviation.
12. A cipher is computationaly secure if
   (a) the cost of breaking it exceeds the value of the information.
   (b) the time of breaking the cipher exceeds the useful lifetime of the information.
   (c) both (a) and (b).
   (d) either (a) or (b).
13. We can show that decryption in the RSA algorithm works because of the theorem invented by?
   (a) Euclid.
   (b) Diffie and Hellman.
   (c) Euler.
   (d) Rivest, Shamir, and Adleman.

14. Which of the following measures is considered under the operational model?
    (a) Login frequency by day and time.
    (b) Failure to login from a specific terminal.
    (c) Frequency of login from different locations.
    (d) Program resource utilization.

Section 2. (5 pts each)

1. Blinding is an operation used against timing attacks in the RSA algorithm. Describe briefely what is done in blinding.

2. In the RSA scheme, assume that Bob had a key but the attacker found out what the private key was (i.e. $KR = (d, n)$). Then Bob new and decided to create a new key from the same n. Is this safe? Explain your answer.

3. Perform encryption and decryption for the RSA algorithm with $p = 5$, $q = 11$, $e = 3$, and $M = 9$.

4. In PGP, the signature is generated before the compression for two reasons. List them briefly.

5. Consider the PGP message format and answer the followin questions:

   Explain why the leading two octets of the message digest is included in the PGP message unencrypted.

   What is the key ID of a key?

   Explain why is the key ID of the receipient's public key is sent. Isn't his public key already known to him.

6. Assuming that Bob's PGP private key was disclosed to an attacker. Bob know's about it and sends a revokation certificate of his key. What is the contents of this certificate?

   Explain why it will not be beneficial for the attacker to send the circtificate himeself and cancel Bob's keys?

7. Describe briefly two different methods for protecting the password file by the operating system.

8. According to the text: "A study of existing intrusion detection systems indicated that existing intrusion detection systems have not overcome the base-rate fallacy". What is the base-rate fallacy in Intrusion Detection Systems? Why is this fallacy harmful to the security of the computer network in an organization?

9. Give two examples of native audit records that may be used by an Intrusion Detection System, and explain how these records can be used to detect an intruder.

Answer Key for Exam A

Section 1.

Circle the most suitable answer for the following questions/statements. (2 points each)

1. The attacker tries every possible key. What is the name of this attack?
   - (a) Chosen plaintext.
   - (b) Known plaintext.
   - (c) Chosen key.
   - [(d)] Brute force.
2. Which of the following algorithms works better when attacking the RSA algorithm?
   - (a) Euclid's algorithm.
   - (b) General number field sieve.
   - [(c)] Special number field sieve.
   - (d) Quadratic sieve.
3. All of the following are strong points of the PGP application except
   - (a) It's available worldwide including its source code.
   - (b) It includes many strong ciphers like DES, AES, Blowfish, IDEA, and CASE-128.
   - [(c)] It provides a key distribution authority for the public keys.
   - (d) It is not controlled by government agencies.
4. Decoy systems that are used to lure potential attackers are called
   - (a) Intrusion Luring Systems.
   - (b) Markov models.
   - (c) Expert systems.
   - [(d)] Honeypots.
5. Which of the following is the most useful and promising password selection strategy?
   - [(a)] Proactive password checking.
   - (b) Reactive password checking.
   - (c) Computer generated passwords.
   - (d) User education.
6. Which of the following is not a polyalphabetic cipher?
   - (a) one-time pad.
   - [(b)] Caeser's cipher.
   - (c) Vigenere's cipher.
   - (d) DES.
7. The design of DES is now considered as vulnerable to attacks because of
   - (a) The number of rounds.
   - (b) The block size.
   - (c) It's too slow.
   - [(d)] The key size.

8. Which of the following modes is useful for high-speed requirements and is provably as secure as the others?

   (a) ECB.
   (b) CBC.
   (c) OFB.
   [(d)] CTR.

9. Which of the following is not considered as a parameter in the design of a Feistel network?

   (a) Subkey generation algorithm.
   (b) Round function.
   [(c)] The exclusive-OR function.
   (d) Block size

10. The permutations done inside the S-box are considered by Shannon as part of the

   [(a)] confusion.
   (b) diffusion.
   (c) both (a) and (b)
   (d) neither (a) nor (b).

11. The simplest measure in statistical anomaly detection is

   (a) Multivatriate measure.
   (b) Markov process.
   (c) Time series analysis.
   [(d)] Mean and standard deviation.

12. A cipher is computationaly secure if

   (a) the cost of breaking it exceeds the value of the information.
   (b) the time of breaking the cipher exceeds the useful lifetime of the information.
   [(c)] both (a) and (b).
   (d) either (a) or (b).

13. We can show that decryption in the RSA algorithm works because of the theorem invented by?

   (a) Euclid.
   (b) Diffie and Hellman.
   [(c)] Euler.
   (d) Rivest, Shamir, and Adleman.

14. Which of the following measures is considered under the operational model?

   (a) Login frequency by day and time.
   [(b)] Failure to login from a specific terminal.
   (c) Frequency of login from different locations.
   (d) Program resource utilization.

Section 2. (5 pts each)

1. Blinding is an operation used against timing attacks in the RSA algorithm. Describe briefely what is done in blinding.

2. In the RSA scheme, assume that Bob had a key but the attacker found out what the private key was (i.e. $KR = (d, n)$). Then Bob new and decided to create a new key from the same n. Is this safe? Explain your answer.

3. Perform encryption and decryption for the RSA algorithm with $p = 5$, $q = 11$, $e = 3$, and $M = 9$.

4. In PGP, the signature is generated before the compression for two reasons. List them briefly.

5. Consider the PGP message format and answer the followin questions:

   Explain why the leading two octets of the message digest is included in the PGP message unencrypted.

   What is the key ID of a key?

   Explain why is the key ID of the receipient's public key is sent. Isn't his public key already known to him.

6. Assuming that Bob's PGP private key was disclosed to an attacker. Bob know's about it and sends a revokation certificate of his key. What is the contents of this certificate?

   Explain why it will not be beneficial for the attacker to send the circtificate himeself and cancel Bob's keys?

7. Describe briefly two different methods for protecting the password file by the operating system.

8. According to the text: "A study of existing intrusion detection systems indicated that existing intrusion detection systems have not overcome the base-rate fallacy". What is the base-rate fallacy in Intrusion Detection Systems? Why is this fallacy harmful to the security of the computer network in an organization?

9. Give two examples of native audit records that may be used by an Intrusion Detection System, and explain how these records can be used to detect an intruder.