CSC 371: Cryptography

Midterm Exam , First semester 2003/2004, Form: A

Name: _____

Student Number: _____

Section: _____

Section 1. (2 points each)

For each question below choose the most appropriate answer and **circle clearly** only one choice of the following questions.

1. Which of the following theorems was used to show that the RSA algorithm's decryption is the reverse of its encryption?
   (a) Euclid's theorem.
   (b) Euler's theorem.
   (c) Einstein's theorem.
   (d) Rivest's theorem.
2. Given a MAC with n-bit output, how long is the input?
   (a) 2^n bits.
   (b) k bits, where $k > n$.
   (c) $2^n - 1$ bits.
   (d) Arbitrary length.
3. Which of the following factorization algorithms is the fastest:
   (a) General Number Field Sieve.
   (b) Special Number Field Sieve.
   (c) Prime Factoring Field Sieve.
   (d) Quadratic Field Sieve.
4. Assume that you would like to find a prime number close to a number n. How many guesses do you have to make on average to find a prime?
   (a) $\log_2(n)$ guesses.
   (b) 2^n guesses.
   (c) $\ln(n/2)$ guesses.
   (d) $\ln(n)/2$ guesses.
5. What does a MAC and/or a hash code protect against?
   (a) Content modification.
   (b) Replay.
   (c) Neither (a) nor (b).
   (d) Both (a) and (b).
6. Which of the following public-key distribution schemes creates more network bottlenecks?
   (a) Public-key authority.
   (b) Public announcement.
   (c) Public-key certificate.
   (d) Public broadcast.

Section 2. (5 points each)

1. Describe a method (you can use a drawing if you like) for authentication without using encryption or a MAC.

   What are the advantages of this scheme over methods which use encryption or MACs for authentication?

2. Consider the following public-key certificate exchange.

   (a) Explain how can B verify the certificate C_A.

   (b) Why do we include a time stamp in the certificate?

3. Consider the following authentication scheme.

   (a) Why can't we use this scheme for authentication in general?

   (b) Which type of messages can be authenticated with this scheme?

4. Given the public-key $KU_a = (27, 55)$, find the private key for A. Show your work.

5. Describe two methods for countering timing attacks on an RSA algorithm.

Answer Key for Exam A

Section 1. (2 points each)

For each question below choose the most appropriate answer and **circle clearly** only one choice of the following questions.

1. Which of the following theorems was used to show that the RSA algorithm's decryption is the reverse of its encryption?
   - (a) Euclid's theorem.
   - [(b)] Euler's theorem.
   - (c) Einstein's theorem.
   - (d) Rivest's theorem.
2. Given a MAC with n-bit output, how long is the input?
   - (a) 2^n bits.
   - (b) k bits, where $k > n$.
   - (c) $2^n - 1$ bits.
   - [(d)] Arbitrary length.
3. Which of the following factorization algorithms is the fastest:
   - (a) General Number Field Sieve.
   - [(b)] Special Number Field Sieve.
   - (c) Prime Factoring Field Sieve.
   - (d) Quadratic Field Sieve.
4. Assume that you would like to find a prime number close to a number n. How many guesses do you have to make on average to find a prime?
   - (a) $\log_2(n)$ guesses.
   - (b) 2^n guesses.
   - (c) $\ln(n/2)$ guesses.
   - [(d)] $\ln(n)/2$ guesses.
5. What does a MAC and/or a hash code protect against?
   - (a) Content modification.
   - (b) Replay.
   - (c) Neither (a) nor (b).
   - [(d)] Both (a) and (b).
6. Which of the following public-key distribution schemes creates more network bottlenecks?
   - [(a)] Public-key authority.
   - (b) Public announcement.
   - (c) Public-key certificate.
   - (d) Public broadcast.

Section 2. (5 points each)

1. Describe a method (you can use a drawing if you like) for authentication without using encryption or a MAC.

   What are the advantages of this scheme over methods which use encryption or MACs for authentication?

2. Consider the following public-key certificate exchange.

   (a) Explain how can B verify the certificate C_A.

   (b) Why do we include a time stamp in the certificate?

3. Consider the following authentication scheme.

   (a) Why can't we use this scheme for authentication in general?

   (b) Which type of messages can be authenticated with this scheme?

4. Given the public-key $KU_a = (27, 55)$, find the private key for A. Show your work.

5. Describe two methods for countering timing attacks on an RSA algorithm.

CSC 371: Cryptography

Midterm Exam , First semester 2003/2004, Form: B

Name: _____

Student Number: _____

Section: _____

Section 1. (2 points each)

For each question below choose the most appropriate answer and **circle clearly** only one choice of the following questions.

1. Which of the following factorization algorithms is the fastest:
   (a) General Number Field Sieve.
   (b) Special Number Field Sieve.
   (c) Prime Factoring Field Sieve.
   (d) Quadratic Field Sieve.
2. Given a MAC with n-bit output, how long is the input?
   (a) 2^n bits.
   (b) k bits, where $k > n$.
   (c) $2^n - 1$ bits.
   (d) Arbitrary length.
3. Assume that you would like to find a prime number close to a number n. How many guesses do you have to make on average to find a prime?
   (a) $\log_2(n)$ guesses.
   (b) 2^n guesses.
   (c) $\ln(n/2)$ guesses.
   (d) $\ln(n)/2$ guesses.
4. Which of the following public-key distribution schemes creates more network bottlenecks?
   (a) Public-key authority.
   (b) Public announcement.
   (c) Public-key certificate.
   (d) Public broadcast.
5. Which of the following theorems was used to show that the RSA algorithm's decryption is the reverse of its encryption?
   (a) Euclid's theorem.
   (b) Euler's theorem.
   (c) Einstein's theorem.
   (d) Rivest's theorem.
6. What does a MAC and/or a hash code protect against?
   (a) Content modification.
   (b) Replay.
   (c) Neither (a) nor (b).
   (d) Both (a) and (b).

Section 2. (5 points each)

1. Describe a method (you can use a drawing if you like) for authentication without using encryption or a MAC.

   What are the advantages of this scheme over methods which use encryption or MACs for authentication?

2. Consider the following public-key certificate exchange.

   (a) Explain how can B verify the certificate C_A.

   (b) Why do we include a time stamp in the certificate?

3. Consider the following authentication scheme.

   (a) Why can't we use this scheme for authentication in general?

   (b) Which type of messages can be authenticated with this scheme?

4. Given the public-key $KU_a = (27, 55)$, find the private key for A. Show your work.

5. Describe two methods for countering timing attacks on an RSA algorithm.

Answer Key for Exam B

Section 1. (2 points each)

For each question below choose the most appropriate answer and **circle clearly** only one choice of the following questions.

1. Which of the following factorization algorithms is the fastest:
   - (a) General Number Field Sieve.
   - (b) Special Number Field Sieve.
   - (c) Prime Factoring Field Sieve.
   - (d) Quadratic Field Sieve.

2. Given a MAC with n-bit output, how long is the input?
   - (a) 2^n bits.
   - (b) k bits, where $k > n$.
   - (c) $2^n - 1$ bits.
   - (d) Arbitrary length.

3. Assume that you would like to find a prime number close to a number n. How many guesses do you have to make on average to find a prime?
   - (a) $\log_2(n)$ guesses.
   - (b) 2^n guesses.
   - (c) $\ln(n/2)$ guesses.
   - (d) $\ln(n)/2$ guesses.

4. Which of the following public-key distribution schemes creates more network bottlenecks?
   - (a) Public-key authority.
   - (b) Public announcement.
   - (c) Public-key certificate.
   - (d) Public broadcast.

5. Which of the following theorems was used to show that the RSA algorithm's decryption is the reverse of its encryption?
   - (a) Euclid's theorem.
   - (b) Euler's theorem.
   - (c) Einstein's theorem.
   - (d) Rivest's theorem.

6. What does a MAC and/or a hash code protect against?
   - (a) Content modification.
   - (b) Replay.
   - (c) Neither (a) nor (b).
   - (d) Both (a) and (b).

Section 2. (5 points each)

1. Describe a method (you can use a drawing if you like) for authentication without using encryption or a MAC.

   What are the advantages of this scheme over methods which use encryption or MACs for authentication?

2. Consider the following public-key certificate exchange.

   (a) Explain how can B verify the certificate C_A.

   (b) Why do we include a time stamp in the certificate?

3. Consider the following authentication scheme.

   (a) Why can't we use this scheme for authentication in general?

   (b) Which type of messages can be authenticated with this scheme?

4. Given the public-key $KU_a = (27, 55)$, find the private key for A. Show your work.

5. Describe two methods for countering timing attacks on an RSA algorithm.