NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758/98065197

Examination date: 2015-08-03

Examination time (from-to): 09:00 - 12:00

Permitted examination support material: (D) No printed or hand-written support material is allowed. A specific basic calculator is allowed.

Other information: –

Language: English

Number of pages: 8

Number of pages enclosed: 1

Checked by:

Date Signature

Instructions

The maximum score is 60 points. The problem set consists of two exercises.

- Exercise 1 consists of the multiple choice questions. There are 20 questions each worth 1 point.

  Answer the multiple choice problems using the separate answer page. The answer page includes answer boxes for multiple choice problems. Check only one box per statement, or no check. If more than one box is checked for a statement, it counts as an incorrect mark.

  Check the boxes like this: ☒

  If you check the wrong box, fill it completely, like this: ■. Then check the correct box.

  Other correction methods are not permitted.

  Incorrect answers receive a discount (penalty) of 0.25 marks,

  Note that the multiple choice problems do not receive penalty marks if you do not check any of the four boxes for a given statement.

- Exercise 2 consists of questions requiring written answers. There are 8 questions, each worth a maximum of 5 points. The written answers should be written in the answer book(s) provided.

Exercise 1 Multiple choice questions

1. A symmetric key cipher must be secure against brute-force key search. A reasonable *minimum* key length for industry-standard security today is:

   (a) 32 bits
   (b) 128 bits
   (c) 512 bits
   (d) 1024 bits

2. Following Kerckhoff's principle, we usually assume that an attacker of an encryption scheme has access to:

   (a) unbounded computational power
   (b) the encryption and decryption keys
   (c) the description of the encryption and decryption algorithms
   (d) all of the above.

3. Triple encryption with DES (triple DES) with three independent keys:

   (a) uses three times as much computation as ordinary DES
   (b) has three times as many possible key values as ordinary DES
   (c) runs three times faster than ordinary DES
   (d) is vulnerable to brute-force key search today

4. The AES (Advanced Encryption Standard) algorithm:

   (a) is based on a Feistel cipher design
   (b) is based on a substitution-permutation network (SPN) design
   (c) was replaced by the Data Encryption Standard (DES) cipher
   (d) was replaced by the Digital Signature Standard (DSS)

5. The inverse of 4 modulo 19 is:

   (a) 1
   (b) 5
   (c) 10
   (d) 15

6. A mode of operation for a block cipher often introduces a random IV. This is useful for security because:

   (a) it adds to the complexity of decryption
   (b) it increases the difficulty of brute-force key search
   (c) the same ciphertext is decrypted to different messages
   (d) the same plaintext is encrypted to different ciphertexts

7. When a message authentication code (MAC) tag is received, in order to check data integrity the recipient needs to:

   (a) decrypt the tag and check for redundancy

   (b) encrypt the tag and check for redundancy

   (c) compare the tag with the tag in the previous message

   (d) recompute the tag and compare with the received tag

8. The one-time pad achieves perfect secrecy. This means that:

   (a) each plaintext is a perfectly random string

   (b) the only feasible attack is brute-force key search

   (c) an attacker cannot alter any bit in the ciphertext without this being detected

   (d) an attacker learns nothing about the plaintext from the ciphertext

9. For numbers of 2048 bits in size there are known efficient algorithms which can be implemented for:

   (a) factorising numbers

   (b) taking discrete logarithms

   (c) generating random prime numbers

   (d) performing exhaustive key search

10. The Fermat test and the Miller–Rabin test are two tests for deciding whether or not a number n is prime. Which of the following statements is true?

    (a) If the Miller–Rabin test outputs *probable prime* then the Fermat test also outputs *probable prime*

    (b) If the Fermat test outputs *probable prime* then the Miller–Rabin test also outputs *probable prime*

    (c) If the Miller–Rabin test outputs *probable prime* then n is definitely prime

    (d) If the Fermat test outputs *probable prime* then n is definitely prime

11. The RSA encryption algorithm uses a public modulus n. Regarding the security of the RSA algorithm it is known that:

    (a) a known plaintext attack allows an attacker to obtain the private key

    (b) finding the plaintext from any ciphertext is as hard as finding the factors of n

    (c) finding the private key from the public key is as hard as finding the factors of n

    (d) quantum computers would not help in an attack

12. The Elgamal encryption algorithm can be broken by an attacker who is able to:

    (a) solve the discrete logarithm problem

    (b) generate large prime numbers

    (c) perform fast exponentiation

    (d) perform a chosen ciphertext attack

13. Public key cryptosystems based on discrete logarithms can be implemented either in elliptic curve groups or in groups of integers modulo a prime p, often written $\mathbb{Z}_p^*$. An advantage of using elliptic curve groups is:

    (a) the cryptosystem is still secure if quantum computers become practical

    (b) shorter public keys can be used to achieve the same security level

    (c) implementation of exponentiation algorithms is simpler

    (d) there are no patent restrictions

14. HMAC is a construction for a message authentication code, often used in TLS. The HMAC algorithm:

    (a) is vulnerable to length extension attacks

    (b) has output size equal to the input size

    (c) uses a single call to the underlying hash function

    (d) can use any iterated hash function

15. When public key cryptography is used to provide digital signatures:

    (a) the public key of the signer is required in order to generate the signature

    (b) the public key of the verifier is required in order to generate the signature

    (c) the private key of the signer is required in order to generate the signature

    (d) the private key of the verifier is required in order to generate the signature

16. A digital certificate is issued by a certification authority. It must include:

    (a) the subject's private key and identity

    (b) the subject's public key and identity

    (c) the certificate authority's private key

    (d) a certificate revocation list

17. In the Kerberos system three kinds of server are involved. A ticket granting ticket (TGT) may be issued by:

    (a) authentication server

    (b) ticket-granting server

    (c) application server

    (d) any type of server

18. Which of the following is *not* explicitly negotiated during the TLS handshake protocol?

    (a) The version of TLS to be used

    (b) The algorithms to be used for exchange of the session key

    (c) The encryption algorithm to be used in the record protocol

    (d) The security services to be provided by the record protocol

19. The TLS sub-protocol concerned with providing confidentiality and integrity to application data is called:

    (a) the handshake protocol

    (b) the record protocol

    (c) the alert protocol

    (d) the change cipher spec protocol

20. One commonly used TLS ciphersuite is denoted as TLS_RSA_WITH_AES_128_CBC_SHA. When this ciphersuite is chosen, RSA is used:

    (a) to sign the server ephemeral Diffie-Hellman value

    (b) to sign the client ephemeral Diffie-Hellman value

    (c) to encrypt the pre-master secret with the server long-term key

    (d) to encrypt the pre-master secret with the client long-term key

Exercise 2 Written answer questions

1. One common way of designing modern block ciphers is to use the Feistel construction. The equations for round i are usually written as follows.

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   (a) Describe what is represented by the values L_i, R_i and K_i in the above equations.

   (b) Write down the corresponding equations used to compute L_{i-1} and R_{i-1}, given L_i and R_i, during decryption.

   (c) Why is it *not* necessary for the function f to be invertible in order to be able to decrypt?

2. One mode of operation for block ciphers is cipher block chaining (CBC). CBC mode can be used either to encrypt the sequence of blocks $P_1, P_2, \ldots, P_n$ or to form a message authentication code (MAC) from the last ciphertext block. The general equation for computing each ciphertext block, where C_0 = IV, is:

$$C_t = E(P_t \oplus C_{t-1}, K)$$

   (a) Suppose first that CBC mode is used for encryption but IV is chosen to be the same for every message. Explain why this is a weakness and how it might be used by an attacker.

   (b) Suppose now that CBC mode is used to form a MAC and now the IV is chosen randomly for each message and sent with the MAC. Explain how an attacker can forge a valid MAC for any one-block message, given a valid MAC on any other one-block message.

3. The Chinese Remainder Theorem (CRT) is often used to speed up decryption in the RSA cryptosystem. If the RSA modulus is $n = pq$, the decryption exponent is d and the ciphertext is C, then the method first computes $M_p = C^{d \bmod p-1} \bmod p$ and $M_q = C^{d \bmod q-1} \bmod q$. Then M_p and M_q are combined with the CRT.

   Illustrate the use of the method for the case where $n = 55 = 5 \times 11$, the decryption exponent is $d = 27$ and the ciphertext is $C = 2$. Specifically, compute M_p and M_q and apply the CRT to find M.

4. In public key cryptography it is often required to compute values of the form $a^b \bmod n$ for some randomly chosen exponent b and large modulus n. This is often achieved using the *square-and-multiply* method.

   (a) Without using any specific values for a or n, illustrate how the square-and-multiply method works by showing the steps required to compute $a^{37} \bmod n$. How many squarings and how many multiplications are needed?

   (b) If n and b are 2000 bits in length, what is the expected number of squarings and multiplications needed to apply the *square-and-multiply* method? How does this vary with different values of b?

5. The Elgamal encryption scheme works in $\mathbb{Z}_p^*$ for a prime p. The public key is $y = g^x \bmod p$ and the private key is the exponent x. To encrypt a message m the ciphertext is the pair $c = (g^k \bmod p, my^k \bmod p)$.

   (a) Explain how an attacker who can take discrete logarithms can find the message from the ciphertext and public key.

   (b) What are reasonable choices today for the size of p which are both secure and reasonably efficient? How will this change if full-scale quantum computers become available?

6. When using the RSA algorithm to form a digital signature, the output is a value $s = h(m)^d \bmod n$ for a suitable hash function h. The message m and s are sent to the verifier.

   (a) Given a valid public exponent e, how does the verifier check the signature?

   (b) Explain how an attacker who can find a *collision* in h can exploit this to construct a message forgery.

7. Consider the following protocol with the goal of key establishment. Here N_A is a nonce chosen by A, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

   1. $A \rightarrow B : ID_A, N_A$
   2. $B \rightarrow S : ID_A, ID_B, N_A$
   3. $S \rightarrow B : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{AS}}, \{K_{AB}, ID_A, ID_B, N_A\}_{K_{BS}}$
   4. $B \rightarrow A : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{AS}}$

   Describe a replay attack on this protocol, showing concrete messages sent by the attacker.

8. Consider the protocol below as an abstract version of the TLS handshake protocol. Client C and server S have negotiated a ciphersuite incorporating ephemeral Diffie-Hellman. The Diffie-Hellman group generator is g and the server certificate is $Cert_S$. The server and client choose random values x and y respectively and the server uses a signature scheme denoted Sig_S.

$$\begin{aligned} S \rightarrow C &: \quad Cert_S, g^x, Sig_S(g^x) \\ C \rightarrow S &: \quad g^y \end{aligned}$$

   (a) Explain how both C and S will compute the TLS session keys.

   (b) Explain why this protocol achieves forward secrecy.

Detach this sheet and hand it in together with your written answers

TTM4135 Examination 2015-08-03
Answer page for Exercise 1 Multiple Choice Questions

Candidate number: □□□□□

1.	(a) □	(b) ☑	(c) □	(d) □
2.	(a) □	(b) □	(c) ☑	(d) □
3.	(a) ☑	(b) □	(c) □	(d) □
4.	(a) □	(b) ☑	(c) □	(d) □
5.	(a) □	(b) ☑	(c) □	(d) □
6.	(a) □	(b) □	(c) □	(d) ☑
7.	(a) □	(b) □	(c) □	(d) ☑
8.	(a) □	(b) □	(c) □	(d) ☑
9.	(a) □	(b) □	(c) ☑	(d) □
10.	(a) ☑	(b) □	(c) □	(d) □
11.	(a) □	(b) □	(c) ☑	(d) □
12.	(a) ☑	(b) □	(c) □	(d) □
13.	(a) □	(b) ☑	(c) □	(d) □
14.	(a) □	(b) □	(c) □	(d) ☑
15.	(a) □	(b) □	(c) ☑	(d) □
16.	(a) □	(b) ☑	(c) □	(d) □
17.	(a) ☑	(b) □	(c) □	(d) □
18.	(a) □	(b) □	(c) □	(d) ☑
19.	(a) □	(b) ☑	(c) □	(d) □
20.	(a) □	(b) □	(c) ☑	(d) □