NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Information Security and Communication Technology

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758 / 98065197

Examination date: 2017-08-08

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: 9

Number of pages enclosed: 2

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 30 questions each worth 1 point.

  Answer the multiple choice problems using the separate answer page. *Detach the answer page and hand it in at the end of the examination with your answers booklet(s).* 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 answer.

  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 0.33 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 6 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. Which of the following integers is a square root of 1 modulo 21?
   - (a) 2
   - (b) 4
   - (c) 6
   - (d) 8

2. The Hill cipher is a historical cipher with the encryption equation $C = KP \bmod n$ for $k \times k$ key matrix K and vectors C and P representing the ciphertext and plaintext. A fundamental weakness of the Hill cipher is:
   - (a) brute force key search is easy for any value of k
   - (b) encryption is a linear function so a known plaintext attack is easy
   - (c) the distribution of ciphertext characters is the same as the distribution of plaintext characters
   - (d) it may not be possible to decrypt a valid ciphertext

3. For which one of the following encryption algorithms are the distributions of plaintext and ciphertext characters the same?
   - (a) The Caesar cipher
   - (b) The random simple substitution cipher
   - (c) A transposition cipher on blocks of size 12
   - (d) The Vigenère cipher with a key of length 8

4. Which of the following is *not* a valid key size for the AES cipher?
   - (a) 128 bit
   - (b) 192 bits
   - (c) 256 bits
   - (d) 512 bits

5. According to Kerkhoff's principle, which of the following should *not* be available to an attacker of an iterated block cipher?
   - (a) The round keys
   - (b) The number of rounds
   - (c) The key length
   - (d) The block length

6. Double DES is the encryption algorithm defined by iterating two instances of the DES algorithm — the initial DES ciphertext is fed back into the encryption algorithm with an independent key. The main disadvantage of double DES is:
   - (a) it is vulnerable to differential cryptanalysis
   - (b) it has poor avalanche effects
   - (c) the key length is too short to resist practical brute-force search
   - (d) there is a meet-in-the-middle attack which reduces the effective key length

7. Which of the following block cipher modes of operation is *not* designed to provide data confidentiality?

   (a) Galois counter mode (GCM)
   (b) Cipher block chaining (CBC)
   (c) Cipher-based MAC (CMAC)
   (d) Counter with CBC-MAC (CCM)

8. Cipher block chaining (CBC) is a mode of operation for block ciphers. Which of the following statements about CBC mode is true?

   (a) Messages to be encrypted must be padded to be a complete number of blocks
   (b) One bit in error in the ciphertext leads to a single bit in error in the decrypted plaintext
   (c) Equal plaintext blocks encrypt to equal ciphertext blocks
   (d) Encryption of a sequence of blocks can be conducted in parallel

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

   (a) each plaintext message 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

10. When using counter mode encryption with a block cipher, a binary keystream is generated by the sender. The keystream generated by the recipient is:

    (a) the same as that generated by the sender
    (b) the complement of that generated by the sender (every bit is different)
    (c) random and independent of that generated by the sender
    (d) random but dependent on the ciphertext received

11. Which of the following pairs of equations *cannot* be solved using the Chinese Remainder Theorem?

    (a) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 17$
    (b) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 17$
    (c) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 18$
    (d) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 18$

12. 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

13. Suppose $n = 187 = 11 \times 17$. According to Euler's Theorem:

    (a) $2^{100} \bmod n = 1$
    (b) $2^{160} \bmod n = 1$
    (c) $2^{186} \bmod n = 1$
    (d) $2^{188} \bmod n = 1$

14. Let g be a generator for the integers modulo p. The discrete logarithm problem is:

    (a) given y, find x with $y = x^g \bmod p$;
    (b) given x, find y with $y = x^g \bmod p$.
    (c) given y, find x with $y = g^x \bmod p$;
    (d) given x, find y with $y = g^x \bmod p$.

15. When public key cryptography is used for encryption:

    (a) the public key of the sender is required in order to encrypt the plaintext
    (b) the public key of the receiver is required in order to encrypt the plaintext
    (c) the private key of the sender is required in order to encrypt the plaintext
    (d) the private key of the receiver is required in order to encrypt the plaintext

16. The RSA encryption scheme often makes use of an algorithm known as OAEP. OAEP is:

    (a) a pre-processing method for messages providing randomness and redundancy
    (b) a symmetric-key encryption algorithm for use in hybrid encryption
    (c) a method to generate large prime numbers efficienctly
    (d) a method to speed up decryption given knowledge of the factors of the modulus

17. For the RSA encryption scheme a large modulus n is chosen, typically around 2048 bits in practice. To improve efficiency, this is often used together with value of:

    (a) $e = 2^{16}$
    (b) $d = 2^{16}$
    (c) $e = 2^{16} + 1$
    (d) $d = 2^{16} + 1$

18. In the basic Diffie-Hellman key exchange protocol, Alice sends $g^a \bmod p$ to Bob, while Bob sends $g^b \bmod p$ to Alice. They compute a shared secret of the form $g^{ab} \bmod p$. A limitation of the basic protocol is that:

    (a) neither Alice nor Bob knows who the key is shared with
    (b) an attacker can easily compute the shared secret from the exchanged messages
    (c) Bob can choose b to make the shared secret have a particular given value
    (d) the values g and p can only be used once

19. Cryptosystems based on the discrete logarithm problem, such as Diffie-Hellman key exchange, can be implemented in the integers modulo a prime p or in an elliptic curve group. Which of the following statements is true?

    (a) There is no known efficient algorithm to find elliptic curve discrete logarithms for quantum computers

    (b) Elliptic curve public keys can have multiple valid private keys

    (c) The square-and-multiply algorithm cannot be used in elliptic curve groups

    (d) Elliptic curve keys can typically be smaller for the same security level

20. The SHA-2 family of hash algorithms includes members which have hash output sizes of:

    (a) 16 bits, 24 bits, 48 bits and 56 bits

    (b) 100 bits, 200 bits, 250 bits and 300 bits

    (c) 64 bits, 128 bits, 224 bits and 256 bits

    (d) 224 bits, 256 bits, 384 bits and 512 bits

21. HMAC is an algorithm often used in TLS and based on a hash function H. Which of these statements with regard to HMAC is true?

    (a) The same secret key must be used to generate and to verify the HMAC tag

    (b) The size of the tag output by HMAC varies with the size of the input message

    (c) The message input to HMAC must be of a fixed length

    (d) The hash function H must have a 256-bit output size

22. A digital signature scheme often applies a hash function to the message to be signed. A *collision* in the hash function can lead to a signature forgery because:

    (a) one message has two different signatures

    (b) one signature is valid for two different messages

    (c) one message has two different hash values

    (d) two different hash values produce the same signature

23. An X.509 digital certificate is issued by a certification authority on behalf of a subject. In order to verify a certificate it is necessary to possess:

    (a) the private key of the subject

    (b) the public key of the subject

    (c) the public key of the certification authority

    (d) the private key of the certification authority

24. One type of key establishment protocol uses *key transport*: the session key is sent from a server to two parties to use to protect future communication. For this type of protocol:

    (a) a replay attack is always possible

    (b) forward secrecy is not possible

    (c) mutual authentication cannot be achieved

    (d) an active adversary can masquerade as any party

25. Kerberos is an authentication service which provides a *single sign-on* solution. This means that:

    (a) a user need only authenticate once in order to access many services during a defined period

    (b) a user needs to authenticate every time access to a server is required

    (c) only a single user is allowed to access a service at any one time

    (d) a single user is able to access services on behalf of other users

26. The purpose of the *handshake protocol* in TLS is to:

    (a) change the cryptographic algorithms from previously used ones

    (b) signal events such as failures

    (c) setup sessions with the correct keys and algorithms

    (d) provide confidentiality and integrity for messages

27. One TLS ciphersuite is denoted as TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. When this ciphersuite is chosen, ECDSA is used:

    (a) to sign the user data

    (b) to sign one or both Diffie–Hellman ephemeral values

    (c) to sign the server certificate

    (d) to sign the client certificate

28. TLS is often used to protect communication between a web browser and a server. A so-called "man-in-the-middle" attack is possible on TLS if the adversary is able to:

    (a) obtain the public key of the server's certification authority

    (b) eavesdrop on the key exchange messages

    (c) install new root certificates in the browser

    (d) obtain previously used session keys

29. PGP is a scheme for email security. One reason for the limited usage of PGP is:

    (a) PGP is not supported by most email servers

    (b) PGP does not allow signing of messages, only encryption of messages

    (c) PGP software is only legally available to US citizens

    (d) PGP users have difficulty in managing their public/private key pairs

30. One common way to apply the IPSec protocol uses a *host-to-gateway* architecture. Which of the following statements about this architecture is true?

    (a) It is typically used to provide secure remote access from a single host

    (b) It is typically used for secure remote management of a single server

    (c) It provides protection for data throughout its transit (end-to-end)

    (d) It is typically used with IPSec in transport mode

Exercise 2 Written answer questions

1. Two examples of historical ciphers are:

   – the simple random substitution cipher;

   – the random transposition cipher;

   Suppose that the alphabet used in each case has 27 characters and that the transposition cipher uses a block of 10 characters.

   (a) How many keys are possible for each of these ciphers? (You can write down an expression – there is no need to give an exact value.)

   (b) Explain how each of these two ciphers can be attacked using a chosen plaintext attack. How much chosen plaintext would be necessary, in each case, to obtain all of the secret key using such an attack?

2. Cipher block chaining (CBC) mode for a block cipher, such as AES, is often used to form a message authentication code (MAC). Consider a different MAC algorithm using the CBC *decryption* equation: the MAC tag for a sequence of blocks $P_1, P_2, \ldots, P_n$ is the last block, T_n, using the following equation, where $P_0 = 00\ldots0$, the block of all zeros.

   $$T_t = D(P_t, K) \oplus P_{t-1}.$$

   (a) Explain how a receiver of the message $P_1, P_2, \ldots, P_n$, who has the shared key K, can check whether the accompanying tag T_n is correct.

   (b) Show that this is *not* a good MAC algorithm by explaining how an attacker can forge a tag on a new message, given a valid tag on a message with multiple blocks.

3. Cryptosystems based on discrete logarithms often make use of a prime number p and a generator g of the integers modulo p, $\mathbb{Z}_p^*$.

   (a) Show that when $p = 13$, the value 2 is a generator but the value 3 is not a generator.

   (b) Consider Diffie–Hellman key exchange in $\mathbb{Z}_p^*$ when $p = 13$ and $g = 2$. If principal A chooses random secret input value $a = 3$ and receives message $y = 8$ from B, what is the shared secret which they both obtain?

4. 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 and the modulus n, how does the verifier check the signature?

   (b) Suppose now that the hash function is not used, so the signature for a message is simply $s = m^d \bmod n$. Explain how an attacker can construct a valid signature and message, without seeing any other signature.

5. Consider the following protocol with the goal of key establishment. Here N_A is a nonce chosen by A, T_B is a timestamp from the clock at S, 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. $A \to S : ID_A, ID_B, N_A$
   2. $S \to A : \{K_{AB}, ID_B, N_A\}_{K_{AS}}, \{K_{AB}, ID_A, T_B\}_{K_{BS}}$
   3. $A \to B : \{K_{AB}, ID_A, T_B\}_{K_{BS}}$

   (a) What is the purpose of including the identity ID_B in the first part of message 2? What attack could happen if it was not included?

   (b) Suppose that an attacker can control the clock at B and set it to any chosen value. Explain how this allows such an attacker can launch a replay attack on the protocol.

6. Two different protocols often used to protect email in transit are PGP and STARTTLS.

   (a) Consider the two following situations.

      i. You want to keep your email contents confidential from your email server.

      ii. You want to hide the *identity* of the person you are sending email to.

      Which of the two protocols can help you in each case? Explain your answers.

   (b) Both of PGP and STARTTLS can use public key cryptography with certified public keys. How do they differ with regard to the way public key certificates are validated?

TTM4135 Examination 2017-08-08
Answer page for Exercise 1 Multiple Choice Questions

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

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) □

TTM4135 Examination 2017-08-08
Answer page for Exercise 1 Multiple Choice Questions

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

Candidate number: □□□□□

21.	(a) □	(b) □	(c) □	(d) □
22.	(a) □	(b) □	(c) □	(d) □
23.	(a) □	(b) □	(c) □	(d) □
24.	(a) □	(b) □	(c) □	(d) □
25.	(a) □	(b) □	(c) □	(d) □
26.	(a) □	(b) □	(c) □	(d) □
27.	(a) □	(b) □	(c) □	(d) □
28.	(a) □	(b) □	(c) □	(d) □
29.	(a) □	(b) □	(c) □	(d) □
30.	(a) □	(b) □	(c) □	(d) □