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: 2018-08-08

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 does *not* have an inverse modulo 21?

   (a) 1
   (b) 2
   (c) 3
   (d) 4

2. ~~A *generator* for $\mathbb{Z}_{21}^*$, has order:~~ The group $\mathbb{Z}_{21}^*$, has order:

   (a) 3
   (b) 7
   (c) 12
   (d) 20

3. 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) the distribution of ciphertext characters is the same as the distribution of plaintext characters
   (c) it may not be possible to decrypt a valid ciphertext
   (d) encryption is a linear function so a known plaintext attack is easy

4. According to Kerkhoff's principle, which of the following should *not* be available to an attacker of an iterated block cipher?

   (a) The number of rounds
   (b) The key length
   (c) The block length
   (d) The round keys

5. Which of the following is *not* a valid description of AES, the Advanced Encryption Standard, algorithm?

   (a) A substitution-permutation network
   (b) A Feistel cipher
   (c) An iterated block cipher
   (d) A product cipher

6. Which of the following is a valid key size for AES, the Advanced Encryption Standard, algorithm?

   (a) 256 bits
   (b) 512 bits
   (c) 1024 bits
   (d) 2048 bits

7. Cipher-based MAC (CMAC) provides which of the following security services?

   (a) Integrity, but not confidentiality

   (b) Both confidentiality and integrity

   (c) Non-repudiation, but not confidentiality

   (d) Both confidentiality and non-repudiation

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

   (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 whole random block in the decrypted plaintext

   (c) Equal plaintext blocks encrypt to equal ciphertext blocks

   (d) Decryption of a sequence of blocks can be conducted in parallel

9. The main practical disadvantage of the one time pad is:

   (a) weak security

   (b) slow encryption performance

   (c) the ciphertext is longer than the plaintext

   (d) the difficulty of managing keys

10. Which of the following statements about binary synchronous stream ciphers is *false*?

    (a) The keystream generated by the sender is the same as the keystream generated by the receiver

    (b) The keystream is dependent on the plaintext

    (c) The encryption operation is the same as the decryption operation

    (d) The ciphertext is dependent on the plaintext

11. 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

12. Suppose $n = 77$. According to Euler's Theorem:

    (a) $2^7 \bmod n = 1$

    (b) $2^{11} \bmod n = 1$

    (c) $2^{60} \bmod n = 1$

    (d) $2^{76} \bmod n = 1$

13. The Chinese Remainder Theorem can be used with the RSA signature algorithm to:

    (a) speed up signing
    (b) speed up verification
    (c) speed up key generation
    (d) protect against attacks using quantum computers

14. Two processes often connected to public key cryptography are integer factorisation and prime generation. With regard to algorithms that we know today (on conventional computers):

    (a) integer factorisation is easier than prime generation for integers of the same length
    (b) prime generation is easier than integer factorisation for integers of the same length
    (c) integer factorisation requires exponential time with respect to the input size
    (d) prime generation requires exponential time with respect to the required output size

15. When public key cryptography is used for encryption:

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

16. The RSA encryption algorithm uses a public exponent e, a private exponent d, and a public modulus n. In order to speed up the encryption process, it is common to:

    (a) choose a small value for e
    (b) choose a small value for d
    (c) apply the Chinese Remainder theorem
    (d) share the same modulus between different users

17. ElGamal encryption in $\mathbb{Z}_p^*$ uses a prime modulus p, while RSA encryption uses a composite modulus n. When p and n are of the same length, and for small plaintexts:

    (a) RSA ciphertexts and Elgamal ciphertexts are the same size
    (b) RSA ciphertexts and Elgamal ciphertexts are of a random size
    (c) RSA ciphertexts are twice the size of Elgamal ciphertexts
    (d) ElGamal ciphertexts are twice the size of RSA ciphertexts

18. In the basic Diffie-Hellman key exchange protocol, Alice sends $A = g^a \bmod p$ to Bob, while Bob sends $B = g^b \bmod p$ to Alice. In order to compute the shared secret, Bob computes:

    (a) $A^b \bmod p$
    (b) $B^a \bmod p$
    (c) $Ag^b \bmod p$
    (d) $Bg^a \bmod p$

19. 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

20. Due to the so-called birthday paradox, we can expect to first find a collision in the SHA-384 hash function after computing around:

    (a) 2^{20} hash values
    (b) 2^{50} hash values
    (c) 2^{192} hash values
    (d) 2^{383} hash values

21. 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 received tag with the tag in the previous message
    (d) recompute the tag and compare with the received tag

22. The GCM algorithm is commonly used in TLS. GCM is:

    (a) an algorithm to compute the strongest ciphersuite shared between client and server
    (b) a MAC construction based on an iterated hash function
    (c) an encryption mode for stream ciphers
    (d) an authenticated encryption mode for block ciphers

23. Digital certificates are signed by a certification authority. In order to make certificate verification as fast as possible, it is common for this purpose to use:

    (a) RSA signatures
    (b) Elgamal signatures
    (c) DSA signatures
    (d) ECDSA signatures

24. An X.509 digital certificate is issued by a certification authority. Which of the following is *not* required to be included in the certificate:

    (a) the subject's private key
    (b) the subject's public key
    (c) the subject's identity
    (d) the expiry date

25. An alternative to a hierarchical PKI is to use a *web of trust*, for example as used by PGP. An important property in a web of trust, that does not apply in a hierarchical PKI, is that:

    (a) private keys can be generated by any party
    (b) public keys can be signed by any party
    (c) subjects can remain anonymous
    (d) a variety of different signature algorithms can be used to sign certificates

26. A valuable security property for key establishment protocols is *forward secrecy*. A protocol with this property ensures that:

    (a) an attacker with access to the current session key cannot obtain previous session keys
    (b) an attacker with access to previous session keys cannot obtain long-term keys
    (c) an attacker with access to long-term keys cannot obtain previous session keys
    (d) an attacker with access to previous session keys cannot obtain the current session key

27. An example of a ciphersuite in TLS is: `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`. When this ciphersuite is used, the role of the block cipher AES is:

    (a) to provide authenticated encryption for handshake data in combination with ECDSA signatures
    (b) to protect application data, running in GCM mode
    (c) to encrypt the elliptic curve Diffie-Hellman key exchange
    (d) to provide an optional alternative to HMAC for application data integrity protection

28. TLS consists of a number of protocols. The protocol responsible for setting up sessions with the correct keys and algorithms is called:

    (a) the record protocol
    (b) the alert protocol
    (c) the change cipher spec protocol
    (d) the handshake protocol

29. STARTTLS is a security protocol often used to protect emails in transit. When used for email protection, STARTTLS:

    (a) can protect confidentiality of email contents from malicious mail servers
    (b) can provide end-to-end security between the sender and recipient
    (c) requires special processing by email clients
    (d) can apply cryptographic protection to metadata such as email headers

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

    (a) It is often used to connect hosts on unsecured networks to resources on secured networks
    (b) A typical application is to securely connect two separate secure networks
    (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 Vigenère cipher;
   - the random transposition cipher.

   Suppose that the alphabet used in each case has 27 characters, that the Vigenère cipher has period 10, and that the transposition cipher uses a block size 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 an attacker can recover the key for each of these two ciphers using a chosen plaintext attack. Would a known plaintext attack be harder in each case?

2. Cipher block chaining (CBC) mode for a block cipher has general equation for computing each output block as:
$$C_t = E(P_t \oplus C_{t-1}, K).$$
   CBC mode is often used to form a message authentication code (MAC), where the MAC tag T is the last block output by the CBC encryption process with a fixed IV. Consider a variant MAC algorithm where the IV is chosen randomly by the sender and included in the tag, so the new tag is (IV, T) and T is still the last CBC encrypted block.

   (a) Explain how a receiver of the message verifies the received tag given the message.

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

3. The RSA encryption algorithm uses a public exponent e, a private exponent d, and a public modulus n.

   (a) If $n = 55$ and $e = 3$ what is the value of d?

   (b) Suppose that users rely on a trusted server S to generate their RSA modulus. To save on computation, S re-uses one prime from each modulus. For example, user U_1 gets modulus $n_1 = pq$, user U_2 gets modulus $n_2 = qr$, and user U_3 gets modulus $n_3 = rs$, for random large primes p, q, r and s. Explain how this would allow an attacker to factorise the modulus of all three users.

4. Several public key cryptosystems work in the group $\mathbb{Z}_p^*$. Suppose that $p = 17$.

   (a) Show that 2 is *not* a generator of $\mathbb{Z}_{17}^*$ but that 3 *is* a generator of $\mathbb{Z}_{17}^*$.

   (b) What is the discrete logarithm of the value 5 in $\mathbb{Z}_{17}^*$ with respect to $g = 3$?

5. The Kerberos protocol makes repeated use of a *ticket*. For example, in the initial interaction with the authentication server, a client C receives a ticket of the form:
$$\{K_{C,tgs}, ID_C, T_1\}_{K_{tgs}}.$$
   where the notation $\{X\}_K$ denotes authenticated encryption of X using key K.

   Explain the purpose of each of each of the three elements $K_{C,tgs}$, ID_C, and T_1. In particular, state what are the consequences if any of them is omitted.

6. The TLS handshake protocol allows negotiation of cryptographic ciphersuites.

   (a) How is the negotiation process implemented within the TLS protocol messages?

   (b) Explain two benefits of allowing such negotiation to occur, in comparison with having a fixed ciphersuite.

   (c) How is the integrity of the negotiation process protected?

   For this question you may restrict your answer to widely used standard versions of TLS (versions 1.0, 1.1 and 1.2).

TTM4135 Examination 2018-08-08
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) ☐
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) ☐