NTNU

Department of Information Security and Communication Technology

Examination paper for TTM4135 Applied Cryptography and Network Security

Academic contact during examination: Anamaria Costache

Phone: 73 55 94 42

Academic contact present at the exam location: NO

Examination date: 2025-08-07

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 (front page excluded): 10

Number of pages enclosed: 0

Informasjon om trykking av eksamensoppgave
Originalen er:
1-sidig ☐ **2-sidig** ☐
sort/hvit ☐ **farger** ☐
skal ha flervalgskjema ☐

Checked by:

_____

Date Signature

Students will find the examination results in Studentweb. Please contact the department if you have questions about your results. The Examinations Office will not be able to answer this.

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 5 questions, each worth a maximum of 6 points. Partial points for each of the questions are divided evenly, so that if there are two parts for a question then each part is worth 3 points and if there are three parts for a questions then each part is worth 2 points.

  The written answers should be written in the answer book(s) provided.

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) 64 bits
   (b) 108 bits
   (c) 128 bits
   (d) 512 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 decryption keys
   (c) The encryption keys
   (d) The description of the encryption and decryption algorithms

3. $2^{-1} \bmod 251$ is equal to:

   (a) 1
   (b) 126
   (c) 250
   (d) 0.5

4. In $\mathbb{Z}_7^*$, the multiplicative group of non-zero integers modulo 7:

   (a) 2 is a generator
   (b) 3 is a generator
   (c) 4 is a generator
   (d) There is no generator

5. In an alphabet of 29 characters, how many possible permutations are there for the random simple substitution cipher?

   (a) 10^{29}
   (b) 2^{29}
   (c) $2 \cdot 10^{29}$
   (d) $29!$

6. 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

7. 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

8. Three-key 3-DES is the block cipher algorithm defined by iterating three instances of the DES algorithm using three independent keys. In contrast to 128-bit key AES, three-key 3-DES:

   (a) Has a shorter key length

   (b) Is the most common choice in TLS ciphersuites

   (c) Has a longer block length

   (d) Is much less efficient for both encryption and decryption

9. In the One-Time Pad (OTP), the key is:

   (a) A random sequence of characters, each of them independently generated

   (b) A random sequence of characters, each of them generated from a seed

   (c) A pseudo-random sequence of characters

   (d) A sequence of characters generated as a function of the message

10. Suppose that 1001100101 is observed to be a ciphertext from the one-time pad using the binary alphabet. Then we know that:

    (a) The plaintext was 1111111111 with probability $1/2^5$

    (b) The plaintext must be different from 1001100101

    (c) The plaintext could have been any 10-bit string

    (d) The keystream used must be different from 1001100101

11. Recall Euler's phi function ϕ. If $n = 99$, what is the value of $\phi(n)$?

    (a) 98

    (b) 30

    (c) 60

    (d) 40

12. For an integer n, when is testing for primality by trial division practical?

    (a) When n is a Mersenne prime

    (b) When n is small

    (c) When n is large

    (d) When n is a palindromic prime

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

    (a) $x \equiv 1 \pmod 7$ and $x \equiv 3 \pmod{25}$

    (b) $x \equiv 5 \pmod{11}$ and $x \equiv 3 \pmod{25}$

    (c) $x \equiv 3 \pmod 5$ and $x \equiv 5 \pmod{11}$

(d) $x \equiv 3 \pmod 5$ and $x \equiv 3 \pmod{25}$

14. Let p be a prime, and g a generator for $\mathbb{Z}_p^*$. The *Discrete Logarithm problem is:*

    (a) Given x, recover y given $y \equiv x \pmod p$

    (b) Given x, recover g given $y \equiv g^x \pmod p$

    (c) Given y, recover x given $y \equiv x^g \pmod p$

    (d) Given y, recover x given $y \equiv g^x \pmod p$

15. The Euler function ϕ is often useful for public key cryptography. For any integer $n > 1$ it is always true that:

    (a) $\phi(n)$ is an odd integer

    (b) $\phi(n)$ divides n

    (c) $\phi(n)$ is an even integer

    (d) $\phi(n) < n$

16. The RSA encryption scheme uses a public exponent e, a private exponent d, and a public modulus n. The relationship between e and d is defined by:

    (a) $e \cdot d \equiv 1 \pmod n$

    (b) $e \cdot d \equiv \phi(n) \pmod n$

    (c) $e \cdot d \equiv 1 \pmod{\phi(n)}$

    (d) $e \cdot d \equiv n - 1 \pmod{\phi(n)}$

17. A typical RSA private key in use today may have length 3072 bits, but a typical symmetric key for the AES block cipher may have length only 128 bits. This longer key for RSA is necessary because:

    (a) Security for public key encryption needs to be stronger than for symmetric key encryption

    (b) RSA keys need to be longer than symmetric keys to avoid attack by quantum computers

    (c) There are more efficient attacks against RSA than brute-force

    (d) Like the One Time Pad (OTP), the key needs to be the same length as the message

18. Due to the birthday paradox, we can expect to find a collision in the SHA-256 hash function after around:

    (a) 2^7 trials

    (b) 2^8 trials

    (c) 2^{128} trials

    (d) 2^{256} trials

19. When public key cryptography is used for digital signatures:

    (a) The public key of the signer is used for signature verification

    (b) The public key of the verifier is used for signature verification

    (c) The private key of the signer is used for signature verification

    (d) The private key of the verifier is used for signature verification

20. The inputs to a public key verification algorithm are:

    (a) The secret verification key, the message m and the signature σ

    (b) The public verification key, the message m and the signature σ

    (c) The public verification key and the hash of the signature σ and message m

    (d) The secret verification key and the hash of the signature σ and message m

21. A difference between a message authentication code (MAC) and a digital signature is:

    (a) A digital signature scheme provides confidentiality but a MAC does not

    (b) A digital signature scheme provides data integrity but a MAC does not

    (c) A digital signature scheme provides non-repudiation but a MAC does not

    (d) A digital signature scheme provides data authentication but a MAC does not

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

    (a) The same message has two different signatures

    (b) Two different messages have the same signature

    (c) One message has two different hash values

    (d) Two different hash values produce the same signature

23. In the basic Diffie-Hellman key exchange protocol, Alice send $A = g^a \pmod p$ to Bob, while Bob send $B = g^b \pmod p$ to Alice. In order to compute the shared secret, on receipt of B, Alice computes:

    (a) $B^a \pmod p$

    (b) $Ag^B \pmod p$

    (c) $A^a \pmod p$

    (d) $AB \pmod p$

24. Consider the group $\mathbb{Z}_{11}^*$ with generator $g = 7$. If $y = 4$ then the discrete logarithm of y, is

    (a) 3

    (b) 4

    (c) 5

    (d) 6

25. The Merkle-Damgård construction for hash functions makes use of a compression function h, which acts on successive message blocks. A benefit of this construction is:

    (a) Computation of a hash value requires a fixed number of calls to h, independent of the length of the input message

    (b) If h is collision-resistant then the whole hash function is collision-resistant

    (c) No padding is required for the input message, no matter what is the output size of h

    (d) The length of the input message does not need to be included

26. The basic ephemeral Diffie–Hellman protocol can be authenticated by adding to each message a digital signature of the sender. The protocol then provides forward secrecy because:

(a) Revealing the Diffie–Hellman shared secret does not reveal the signing keys

(b) Revealing the signing keys does not reveal the Diffie–Hellman shared secret

(c) Revealing the Diffie–Hellman ephemeral secret keys does not reveal the Diffie–Hellman shared secret

(d) Revealing the Diffie–Hellman ephemeral secret keys does not reveal the signing keys

27. One valid TLS 1.2 ciphersuite is denoted as

    TLS_RSA_WITH_AES_128_CBC_SHA256.

    When this ciphersuite is chosen, integrity of application data is provided by:

    (a) An HMAC tag with SHA-256 as the underlying hash function

    (b) A CBC-based tag with AES as the underlying encryption function

    (c) Signing each application message with an RSA signature

    (d) Appending a hash of each packet, using SHA-256, before encryption with AES

28. PGP is a security protocol to protect emails in transit. Which of the following statements about PGP is true:

    (a) It provides confidentiality of metadata such as email headers

    (b) It provides end-to-end security between the sender and recipient

    (c) It requires special processing by email servers during email transit

    (d) It uses hierarchical digital certificates as also used in HTTPS

29. 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

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

Written answer questions

1. The Hill cipher is a historical cipher with the encryption equation $C = KP \pmod{n}$ for key matrix K and column vectors C and P representing the ciphertext and plaintext respectively. Here n is the size of the alphabet in use. In this question we consider the 2×2 Hill cipher.

   (a) What is the exact number of keys possible?

   (b) Explain what is meant by a chosen plaintext attack and chosen ciphertext attack on the Hill cipher.

   (c) How could you run a ciphertext-only attack (hint: think of using pairs of characters)?

2. One mode of operation for block ciphers is cipher block chaining mode (CBC). The general equation for computing each output block is:

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

   where $C_0 = IV$ which is sent with the ciphertext. The notation $A \oplus B$ denotes bitwise exclusive-OR of blocks A and B.

   (a) In order to save on bandwidth, two parties A and B agree beforehand on a fixed IV to be used for every message which they exchange. Discuss the security implications.

   (b) Suppose that there is an error in transmission when block C_t is sent to a recipient, so that one bit is changed. How many blocks, or partial blocks, are changed when the receiver decrypts? Explain your answer.

   (c) Is it possible to *encrypt* multiple plaintext blocks in parallel? Is it possible to *decrypt* multiple blocks in parallel? Explain your answers.

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 nwhere $n = 65 = 5 \times 13$, $p = 5$, $q = 13$, the decryption exponent is $d = 5$ and the ciphertext is $C = 2$. Specifically,

   (a) Compute M_p and M_q.

   (b) Apply the CRT to recover M.

   (c) Can the CRT be used to speed up decryption? How? Explain your reasoning.

   Show your working to illustrate how the CRT is used and how each component is derived.

4. 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 $p = 11$, the value $g = 7$ is a generator but the value $g = 3$ is not.

   (b) Consider Diffie–Hellman key exchange in $\mathbb{Z}_p^*$ when $p = 11$ and $g = 7$. If A chooses random secret input value $a = 8$ and receives message $y = 5$ from B, what is the shared secret which they both obtain?

5. Recently it has been widely suggested that secure communications on the Internet should provide forward secrecy.

(a) Describe what attack forward secrecy prevents when provided on a TLS connection.

(b) How could a web server ensure that all TLS connections it establishes with clients provide forward secrecy?

(c) The TLS handshake protocol is complex and allows several variants. In this question we focus on the TLS 1.3 version of the handshake protocol. Describe one improvement of TLS 1.3 over TLS 1.2.

TTM4135 Examination 2025-08-07
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) ☐