NTNU – Trondheim
Norwegian University of
Science and Technology

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

Examination date: 2024-05-24

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: 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 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. Which of the below represents a passive threat:

   (a) Replay
   (b) Denial of Service
   (c) Traffic analysis
   (d) Masquerade

2. $2^{-1} \bmod 355$ is equal to:

   (a) 1
   (b) 178
   (c) 350
   (d) 0.5

3. In $\mathbb{Z}_{11}^*$, the multiplicative group of non-zero integers modulo 11:

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

4. In an alphabet of 32 characters, how many possible permutations are there for the random simple substitution cipher?

   (a) 10^{32}
   (b) 2^{32}
   (c) $2 \cdot 10^{32}$
   (d) $32!$

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. 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

8. Suppose that 10011 is observed to be a ciphertext from the one-time pad using the binary alphabet. Then we know that:

   (a) The plaintext was 11111 with probability $1/2^5$

   (b) The plaintext must be different from 10011

   (c) The plaintext could have been any 5-bit string

   (d) The keystream used must be different from 10011

9. Recall Euler's phi function ϕ. If $n = 105$, what is the value of $\phi(n)$?

   (a) 99

   (b) 104

   (c) 48

   (d) 47

10. 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

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

    (a) $x \equiv 1 \pmod 7$ and $x \equiv 3 \pmod{17}$

    (b) $x \equiv 5 \pmod 8$ and $x \equiv 3 \pmod{17}$

    (c) $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod{18}$

    (d) $x \equiv 3 \pmod 8$ and $x \equiv 5 \pmod{18}$

12. 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 $y \equiv g^x \pmod p$

13. 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) $\phi(n) < n$

14. Algorithms for testing the primality of an integer n sometimes result in obtaining a non-trivial square root of 1 modulo n. Knowledge of such a value:

    (a) allows n to be factorised

    (b) shows that n is prime

    (c) shows that $n - 1$ is prime

    (d) shows that $n + 1$ is prime

15. What do "Harvest now, decrypt later" attacks refer to?

    (a) An attack where we collect TLS data on-the-fly, then decrypt later

    (b) An attack where we collect data, and run a supercomputer in the background to decrypt

    (c) An attack where we collect data now, and decrypt with when a large enough quantum computer becomes available

    (d) Any kind of attack where we collect data, then decrypt it in an offline phase

16. When public key cryptography is used for encryption:

    (a) The private key of the sender is needed during encryption

    (b) The private key of the recipient is needed during encryption

    (c) The private key of the sender is needed during decryption

    (d) The private key of the recipient is needed during decryption

17. 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

18. 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

19. In a public key signature scheme, the *unforgeability* property refers to the fact that is is impossible to:

    (a) Construct a pair (m, σ) that passes verification without the public verification key K_s

    (b) Construct a pair (m, σ) that passes verification without the secret verification key K_s

    (c) Construct a pair (m, σ) that passes verification without the public signing key K_s

    (d) Construct a pair (m, σ) that passes verification without the secret signing key K_s

20. A message authentication code (MAC) requires a key as input while a hash function does not. Because of this:

    (a) It is always easy to find collisions for a MAC

    (b) The output size of a MAC must be longer than the output size of a hash function for the same security level

(c) A MAC must be more efficient to compute than a hash function

(d) A MAC can provide data integrity

21. Two commonly used signature schemes are RSA signatures and DSA signatures. In practical implementations, and at the same security level:

(a) RSA signatures are faster to generate

(b) RSA signatures are shorter

(c) RSA signatures are faster to verify

(d) RSA signatures perform all computations with a shorter modulus

22. A cryptographic hash function h often needs the property of collision resistance. To ensure that finding collisions is of the same order of difficulty as brute force key search on a symmetric cipher with a key of 128 bits, the output size of h should be approximately:

(a) 256 bits

(b) $\sqrt{128}$ bits

(c) 64 bits

(d) 128 bits

23. A plaintext P is encrypted into a ciphertext C with a one-time pad. Suppose that an attacker is able to mount a known plaintext attack to obtain a portion of P and the corresponding portion of C. This enables the attacker to obtain:

(a) Nothing except what the attacker could obtain in a ciphertext only attack

(b) A portion of the keystream

(c) The whole keystream

(d) The whole plaintext P

24. Which of the following is a valid key size for the Advanced Encryption Standard (AES)?

(a) 256 bits

(b) 512 bits

(c) 1024 bits

(d) 2048 bits

25. An advantage of cipher block chaining (CBC) mode for a block cipher, in comparison to electronic code book (ECB) mode, is that:

(a) CBC mode protects against dictionary attacks but ECB mode does not

(b) CBC mode protects against brute force key search but ECB mode does not

(c) CBC mode protects against replay attacks but ECB mode does not

(d) CBC mode protects against chosen plaintext attacks but ECB mode does not

26. Three modes of operation for block ciphers are ECB mode, CBC mode and CTR mode. Consider the size of encrypted messages for each mode, measured as the total number of bits that must be communicated. Suppose that the nonce used in CTR mode is half the size of the block size. Which of the following is then true for any size of message?

(a) CTR mode always needs to communicate more bits than CBC mode

(b) CTR mode always needs to communicate more bits than ECB mode

(c) ECB mode always needs to communicate more bits than CBC mode

(d) CBC mode always needs to communicate more bits than ECB mode

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. An X.509 digital certificate is issued by a certification authority C for a subject A. Which of the following *must* be included in the certificate:

    (a) The private key of A

    (b) The private key of C

    (c) A signature of A

    (d) A signature of C

29. In the TLS 1.2 handshake protocol, the last message from the server is called the Server Finished message and includes a checksum over all of the previous handshake messages. If the client did not check the integrity of this message then an attacker could:

    (a) Alter the ciphersuite agreed for this session

    (b) Masquerade as the server

    (c) Obtaine the agreed pre-master secret

    (d) Obtain the session key

30. A difference between TLS 1.3 and TLS 1.2 is:

    (a) The TLS 1.3 handshake protocol always provides forward secrecy

    (b) There are no known attacks on the TLS 1.3 protocol

    (c) The TLS 1.3 record protocol includes data compression

    (d) The TLS 1.3 protocol provides post-quantum security

Written answer questions

1. Frequency analysis is effective in cryptanalysis of historical ciphers. This can include frequency of individual characters, pairs of characters (digrams) and sequences of three characters (trigrams). Consider the following three ciphers when they are used to encrypt plaintext from a natural language, such as English:

   – the 3×3 Hill cipher, with encryption algorithm $C = KP$ where the key K is an invertible 3×3 matrix;

   – random simple substitution cipher, which permutes the alphabet of characters;

   – simple transposition, which permutes blocks of plaintext characters – assume that blocks have at least 10 characters.

   (a) How many keys are possible for each of these ciphers (you only need to write down a formula)?

   (b) For the case of the 3×3 Hill cipher, how could you run a ciphertext-only attack (hint: think of using pairs of characters)? For the other two, how could you run a chosen plaintext attack, and how many chosen plaintext would be necessary?

2. Consider a non-standard mode of operation for block ciphers, similar to, but different from, CTR mode. It has the following general equation for computing each output block:

   $$C_t = O_t \oplus P_t \oplus C_{t-1}$$

   where $O_t = E(T_t, K)$ and $T_t = N \| t$ is the concatenation of a nonce N and block number t, and $C_0 = 0$ (the block of all 0 bits). The notation $A \oplus B$ denotes bitwise exclusive-OR of blocks A and B.

   (a) What is the equation for decryption of ciphertext block C_t to obtain the plaintext block P_t?

   (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 where $n = 55 = 5 \times 11$, the decryption exponent is $d = 11$ and the ciphertext is $C = 2$. Specifically,

   (a) Compute M_p and M_q

   (b) Apply the CRT to find 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 $p = 17$, the value 2 is not a generator but the value 3 is a generator.

(b) Consider Diffie–Hellman key exchange in $\mathbb{Z}_p^*$ when $p = 17$ and $g = 3$. If A chooses random secret input value $a = 3$ and receives message $y = 4$ from B, what is the shared secret which they both obtain?

5. 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.

(a) It is optional for a client to use a certificate. What are the security consequences when a client does *not* have a certificate?

(b) TLS 1.3 offers several different ciphersuites which are negotiated in the handshake. State and explain one advantage and one disadvantage of allowing different ciphersuites.

(c) How does 0-RTT enhance the protocol compared to TLS1.2? Are there any security trade-offs?

TTM4135 Examination 2023-06-08
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) ☐