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: Colin Boyd

Phone: 98065197

Examination date: 2023-06-08

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

   (a) 1

   (b) 126

   (c) 250

   (d) 0.5

2. 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

3. Consider the following historical ciphers used to encrypt English plaintext with a 26-letter alphabet. Which of the following is expected to have the most smooth (uniform) single character frequencies in its ciphertext?

   (a) Caesar cipher

   (b) random simple substitution

   (c) Vigenère cipher with period 5

   (d) Vigenère cipher with period 10

4. Suppose $C = E(P, K)$ denotes encryption of plaintext P with key K to obtain ciphertext C. In a *known plaintext attack*, which of the following is available to an attacker?

   (a) Some previous valid plaintext-ciphertext pair (P, C)

   (b) The key K

   (c) The ciphertext corresponding to the encryption of a plaintext P chosen by the attacker

   (d) The plaintext corresponding to the decryption of a ciphertext C chosen by the attacker

5. Which of the following features of the one time pad is shared by a block cipher in counter (CTR) mode?

   (a) The key must be as long as the plaintext

   (b) A change in one ciphertext bit results in one changed bit in the decrypted plaintext

   (c) Perfect secrecy is achieved

   (d) The key must be perfectly random

6. Which of the following statements about binary synchronous stream ciphers is true?

   (a) Each bit in the keystream of the receiver is different from the corresponding bit in the keystream of the sender

   (b) The keystream depends on the plaintext

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

   (d) The modulo 2 sum (XOR) of the keystream and the ciphertext must be the all zero string

7. Which of the following is *not* a valid description of the Advanced Encryption Standard (AES)?

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

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

   (a) 128 bits
   (b) 512 bits
   (c) 1024 bits
   (d) 2048 bits

9. In the simplest mode of operation for block ciphers, ECB, blocks are encrypted independently. Why do we usually prefer to use a different mode?

   (a) To ensure that identical plaintext blocks encrypt to different ciphertext blocks
   (b) To reduce computational effort
   (c) To allow parallel encryption
   (d) To increase the difficulty of brute force key search

10. Suppose that you have a message of 150 bits to encrypt and you choose to use the AES block cipher. Which of the following modes of operation will require the least number of sent bits in the encrypted message?

    (a) ECB mode
    (b) Counter mode with a nonce of 64 bits
    (c) CBC mode
    (d) GCM mode

11. A cryptographic hash function h often needs to have 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 256 bits, the output size of h should be of size approximately:

    (a) 128 bits
    (b) 184 bits
    (c) 256 bits
    (d) 512 bits

12. The GCM mode of operation for block ciphers provides which of the following security services?

    (a) Integrity, but not confidentiality
    (b) Both integrity and confidentiality
    (c) Non-repudiation, but not confidentiality
    (d) Both non-repudiation and confidentiality

13. When the Miller–Rabin test is used to test the primality of an integer n, it is possible that a non-trivial square root of 1 modulo n is discovered. When this happens:

    (a) we know that n is prime

    (b) we know that n is composite

    (c) the test has failed and must be run again

    (d) the result is not yet decided so the test must continue

14. Suppose $n = 55$. Then, by Euler's Theorem,

    (a) $3^{10} \bmod n = 1$

    (b) $3^{30} \bmod n = 1$

    (c) $3^{40} \bmod n = 1$

    (d) $3^{50} \bmod n = 1$

15. Suppose that a cryptographic system uses both elliptic curve cryptography and AES. If AES is implemented with 192-bit keys, to achieve a similar level of security, the elliptic curve group chosen should have size at least 2^n where n has:

    (a) 128 bits

    (b) 192 bits

    (c) 384 bits

    (d) 512 bits

16. The RSA encryption scheme computes $C = M^e \bmod n$ (where message M is suitably pre-processed). Decryption with private key d correctly recovers M from C because:

    (a) $M^{e+d} \bmod n = M$

    (b) $M^{e+d} \bmod \phi(n) = M$

    (c) $M^{ed} \bmod n = M$

    (d) $M^{ed} \bmod \phi(n) = M$

17. The RSA encryption scheme uses a public exponent e and a private exponent d, together with a modulus n. It is common to fix e to be the value $e = 2^{16} + 1$. To make decryption efficient we could instead choose $d = 2^{16} + 1$, but this is never done because:

    (a) the Chinese Remainder Theorem could not be used

    (b) the decryption process would fail

    (c) the encryption process would take exponential time as a function of the length of n.

    (d) d must be kept secret for security reasons

18. OAEP is a coding algorithm often used together with RSA encryption. Using OAEP helps to:

    (a) prevent dictionary attacks

    (b) allow longer messages to be encrypted

    (c) speed up encryption

    (d) speed up decryption

19. The basic Diffie-Hellman key exchange protocol can run in $\mathbb{Z}_p^*$ or in an elliptic curve group (ECDH) with group generator G. For ECDH, we normally write the group operation as addition so that Alice sends $A = aG$ to Bob, and Bob sends $B = bG$ to Alice. Then, to generate the shared secret, Bob computes:

    (a) $aA + bG$

    (b) $aB + bG$

    (c) aB

    (d) bA

20. 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

21. RSA signatures use a composite modulus n while DSA signatures use a prime modulus p and an element g of order q, where q divides $p - 1$. When n and p are of the same length:

    (a) RSA signatures are shorter than DSA signatures

    (b) DSA signatures are shorter than RSA signatures

    (c) RSA signatures are the same size as DSA signatures

    (d) RSA signatures can be longer, shorter, or equal in length to DSA signatures

22. TLS is today commonly implemented with signatures on elliptic curves, known as ECDSA signatures. Which of the following statements about ECDSA signatures is true?

    (a) They are secure against quantum computers

    (b) They are half the size of DSA signatures for the same security level

    (c) Both the public and private keys are elliptic curve points

    (d) They usually employ one of a standardised set of elliptic curves

23. 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

24. 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

25. Two possible variants of the handshake protocol in TLS 1.2 are based on (i) RSA encryption and (ii) elliptic curve Diffie-Hellman (ECDH). An advantage of using the ECDH variant is:

    (a) the TLS *server key exchange* message is shorter for the same security level

    (b) the handshake protocol is secure against quantum computers

    (c) forward secrecy for the session is provided

    (d) no server certificate is needed

26. 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

27. TLS 1.3 aims to establish secure connections faster than TLS 1.2. One difference between the protocols which contributes to this is that in TLS 1.3:

    (a) clients are not required to verify server certificates

    (b) servers can initiate the handshake protocol and use a ciphersuite of their choice

    (c) clients can send their keyshare field before the ciphersuite is agreed

    (d) some handshake messages are sent encrypted

28. 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 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 security for data throughout its transit (end-to-end)

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

29. Security of email can be improved by using a client system such as Pretty Good Privacy (PGP) or a node-to-node system such as opportunistic TLS (StartTLS). An advantage of using PGP over using StartTLS is that:

    (a) network entities need not be trusted to maintain email content confidentiality

    (b) confidentiality of email header information is always provided

    (c) forward secrecy of email content is always provided

    (d) email clients require no special configuration

30. The secure messaging system, Signal, achieves the property of *post-compromise security*, also known as *self healing*. The cryptographic mechanism used to achieve this is:

    (a) authenticated encryption of message contents

    (b) pre-computed Diffie-Hellman keys

    (c) continuous key exchange with the Diffie–Hellman ratchet

    (d) the symmetric ratchet using hashing

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) For each of these three ciphers, describe how similar or different we can expect the distribution of *trigrams* in the ciphertext to be to the trigram distribution in the plaintext. You may decide whether to count trigrams overlapping or non-overlapping.

   (b) For the case of the 3×3 Hill cipher, how could you use the trigram frequency distribution to help in a ciphertext-only attack?

2. A standardised deterministic random bit generator (DRBG) uses a block cipher E in CTR mode. The output block of the DRBG at instance t is defined by:

$$O_t = E(S_t, K) \tag{1}$$

   where S_t is the current state and K the current key. Both S_0 and K are defined in an initialisation process while S_{t+1} is defined by incrementing state S_t (adding 1 as an integer).

   (a) If E is a good block cipher, why is it reasonable to assume that the output from O_t and O_{t+1} are completely different?

   (b) Suppose that the system is compromised at instance t, so that both S_t and K become known to the attacker. Explain, with reasoning, which output blocks the attacker can then obtain.

   (c) Suppose now that after every 100 output blocks, a standard one-way hash function h is run to update the key to a new value: $K' = h(K)$. The generator then continues as defined in equation (1) with K' replacing K. How does this change your answer to part (b) above?

Continued on next page

3. Suppose that a company generates an RSA public key, (e, n), with private exponent d, to allow external parties to send confidential messages. To increase security inside the company, the private exponent d is split into two parts d_1 and d_2 by choosing d_1 randomly in the range $1 < d_1 < n$, and d_2 so that

$$d = (d_1 + d_2) \bmod \phi(n).$$

Then d_1 is given to one manager and d_2 is given to a second manager and d is deleted. To encrypt message M, external parties compute $C = M^e \bmod n$ as usual for RSA. To decrypt ciphertext C, the managers separately compute $M_1 = C^{d_1} \bmod n$ and $M_2 = C^{d_2} \bmod n$ and then combine their results to obtain $M = M_1 M_2 \bmod n$.

(a) Show that correctly encrypted messages will be correctly decrypted by the above method. You may assume that normal RSA decryption works correctly.

(b) Discuss whether an attacker gains any advantage by learning just one of the two parts d_1 and d_2.

(c) Can the Chinese Remainder Theorem be used to speed up decryption for each of the managers? Explain your answer.

4. Two common types of long-term certified public key in use by servers running TLS are (i) RSA keys and (ii) ECDSA keys.

(a) Suppose that a server is running TLS 1.2 and supports ciphersuites which use RSA key transport as well as ciphersuites which use signed Diffie-Hellman. Compare the advantages of using an RSA key at the server with the advantages of using an ECDSA key at the server.

(b) Why are ECDSA keys more suitable to use in TLS 1.3 than in TLS 1.2?

5. Forward secrecy is often achieved in key establishment protocols by using the Diffie–Hellman protocol. However, many network protocols, such as email or messaging, cannot guarantee interaction needed for ephemeral Diffie-Hellman because message recipients may not be online when the message is sent.

(a) The Signal protocol makes use of pre-distributed keys in order to start the Diffie-Hellman exchange. To what extent does this solution provide forward secrecy equivalent to use of interactive Diffie-Hellman?

(b) Another technique used by Signal is to update the current message key by hashing it, when consecutive messages are sent in the same direction. If the current message key becomes compromised and known to the attacker, how many messages could the attacker recover?

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) □