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: 2018-06-04

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. What is $8^{-1} \bmod 21$?

   (a) 1
   (b) 2
   (c) 4
   (d) 8

2. A *generator* for $\mathbb{Z}_{15}^*$, has order:

   (a) 1
   (b) 3
   (c) 8
   (d) 14

3. If a plaintext comes from a natural language, such as English, for which of the following ciphers is the frequency of any particular character equal in both plaintext and ciphertext?

   (a) The Caesar cipher
   (b) The random simple substitution cipher
   (c) A transposition cipher on blocks of size 12
   (d) The Vigenére cipher with a key of length 8

4. Which is the smallest of the following key sizes that would be acceptable to prevent exhaustive key search today?

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

5. AES, the Advanced Encryption Standard, algorithm:

   (a) has a 128 bit block size
   (b) has a 192 bit block size
   (c) has a 256 bit block size
   (d) allows any of the above block sizes

6. Each round of the AES algorithm:

   (a) performs a substitution on a complete block
   (b) operates on multiple blocks at the same time
   (c) performs a non-linear operation
   (d) uses the same key bits

7. Galois counter mode (GCM) 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. Counter mode (CTR) is a mode of operation for block ciphers. Which of the following statements about CTR 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 one bit in error in the decrypted plaintext
   (c) Repeated plaintext blocks encrypt to different ciphertext blocks
   (d) Encryption of a sequence of blocks can be conducted in parallel

9. The one time pad:

   (a) provides data integrity
   (b) provides perfect secrecy
   (c) produces ciphertext which is twice the length of the plaintext
   (d) requires much more computation for encryption than for decryption

10. According to the relevant NIST standard, a secure Deterministic Random Bit Generator (DRBG) should prevent an attacker from:

    (a) reliably distinguishing the output of the DBRG from a truly random string
    (b) correctly predicting the next output bit with probability at least 1/2
    (c) observing any output from the DBRG
    (d) choosing its own seed and observing the output from the DBRG

11. Which of the following pairs of equations *can* be solved using the Chinese Remainder Theorem?

    (a) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 8$
    (b) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 10$
    (c) $x \equiv 3 \bmod 7$ and $x \equiv 4 \bmod 12$
    (d) $x \equiv 3 \bmod 7$ and $x \equiv 4 \bmod 14$

12. By Euler's theorem, if $\gcd(a, n) = 1$ then it is always true that:

    (a) $a^{n-1} \bmod \phi(n) = 1$
    (b) $a^{n-1} \bmod n = 1$
    (c) $a^{\phi(n)} \bmod \phi(n) = 1$
    (d) $a^{\phi(n)} \bmod n = 1$

13. The Fermat test can be used to decide whether or not a number n is prime. The test can sometimes fail with the result that:

    (a) a prime number is labelled as a composite number

    (b) a composite number is labelled as a prime number

    (c) the test halts without producing any output

    (d) the test continues computing without producing a result

14. Suppose that a cryptographic system uses both RSA and AES. If AES is implemented with 128-bit keys, to achieve a similar level of security, RSA should use a modulus of size:

    (a) 1024 bits

    (b) 3072 bits

    (c) 7680 bits

    (d) 15360 bits

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

    (a) the public key of the signer is required in order to sign a message

    (b) the public key of the verifier is required in order to sign a message

    (c) the private key of the signer is required in order to sign a message

    (d) the private key of the verifier is required in order to sign 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 decryption 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. When the RSA encryption scheme is implemented according to current best practice, the best known attack currently available is to:

    (a) make a brute force search for d

    (b) find the discrete log of the ciphertext

    (c) factorise $\phi(n)$

    (d) factorise n

18. In the ElGamal encryption scheme, a ciphertext for message m has two parts: $C_1 = g^k \bmod p$ and $C_2 = my^k \bmod p$, where $y = g^x$ is the recipient public key. In order to recover the message, the recipient must compute:

    (a) $C_1 \cdot (C_2^x)^{-1} \bmod p$

    (b) $C_2 \cdot (C_1^x)^{-1} \bmod p$

    (c) $C_1^x \cdot (C_2)^{-1} \bmod p$

    (d) $C_2^x \cdot (C_1)^{-1} \bmod p$

19. Consider the group $\mathbb{Z}_p^*$ with generator g. If $y = g^x \bmod p$ then an instance of the discrete logarithm problem is to:

    (a) compute y given p, g and x

    (b) compute g given p, y and x

    (c) compute p given y, g and x

    (d) compute x given p, g and y

20. Suppose that an attacker has the ability to compute the output of a certain hash function for 2^{128} input values. In order to prevent the attacker from finding a collision in the hash function, the output of the hash function should be of length at least:

    (a) 128 bits

    (b) 256 bits

    (c) 384 bits

    (d) 512 bits

21. A message authentication code (MAC) takes as input a message and a key and outputs a tag. To be considered secure a MAC should have the property:

    (a) the correct tag for a new message cannot be computed without the key

    (b) the message used to compute the tag cannot be distinguished from a random message

    (c) different tags are computed if a message is repeated

    (d) any output tag cannot be distinguished from a random string

22. Which of the following algorithms is commonly used in TLS to provide authenticated encryption?

    (a) AES in counter mode

    (b) SHA-256

    (c) HMAC

    (d) GCM

23. Two commonly used digital signatures schemes are RSA signatures and ECDSA. RSA is commonly used to sign digital certificates. This is because, for the same security level:

    (a) RSA public key lengths are shorter

    (b) RSA signatures are shorter

    (c) RSA signature generation is faster

    (d) RSA signature verification is faster

24. An X.509 digital certificate is issued by a certification authority. In order to verify such a certificate it is necessary, in addition to the certificate itself, to have:

    (a) the subject's private key

    (b) the subject's public key

    (c) the certification authority's private key

    (d) the certification authority's public key

25. The basic ephemeral Diffie–Hellman protocol can be strengthened by adding to each message a digital signature of the sender. The effect of this on the protocol is to:

    (a) provide entity authentication

    (b) allow shorter Diffie–Hellman parameters

    (c) prevent replay attacks

    (d) prevent attacks which can find discrete logarithms

26. When assessing the security of a key establishment protocol, such as the Needham–Schroeder protocol, we assume that an attacker is *not* able to:

    (a) obtain session keys used in any previous runs of the protocol

    (b) obtain long-term keys of the parties in the protocol run under attack

    (c) obtain messages exchanged between honest parties in the protocol run under attack

    (d) replay messages used in previous protocol runs

27. 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 application messages

28. When TLS is used to protect web browser communications with HTTPS, a man-in-the-middle (MITM) attack is possible if an attacker is able to:

    (a) masquerade as a network node

    (b) add root certificates into the browser

    (c) obtain a valid server certificate

    (d) alter the `hello` messages in the TLS handshake

29. 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

30. One common way to apply the IPSec protocol uses a *host-to-host* 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 tunnel mode

Exercise 2 Written answer questions

1. The Hill cipher is a historical cipher with the encryption equation $C = KP \bmod n$ 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 2x2 Hill cipher.

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

   (b) Explain how an attacker can use a chosen plaintext attack to obtain the key with just two chosen plaintext pairs.

   (c) Will a similar *chosen ciphertext attack* also work? Explain your answer.

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.

   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.

   (a) Why is this a bad idea in general?

   (b) Suppose that an attacker wants to check whether a captured ciphertext sent from A to B has first plaintext block equal to a particular block P_1. How can this be achieved with a chosen plaintext attack?

3. The RSA encryption algorithm uses a public exponent e, a private exponent d, and a public modulus n. The basic equation for encryption is $c = m^e \bmod n$

   (a) If $n = 21$ and $d = 5$ what is the value of e? What is the ciphertext if $m = 3$?

   (b) In order to make key generation more efficient, suppose that A and B use a trusted server S to generate a shared modulus n. S then chooses distinct random private keys, d_A and d_B, and computes corresponding e_A and e_B values. S securely sends the values d_A and d_B to A and B respectively and makes e_A, e_B and n public. Explain how this would allow A to find the private key, d_B, of B.

4. Diffie–Hellman key exchange can work in the group $\mathbb{Z}_p^*$. Suppose that $p = 13$ and $g = 2$ are used.

   (a) Show that $g = 2$ is a generator of $\mathbb{Z}_{13}^*$.

   (b) What is the value of the shared secret if Alice sends the value 3 to Bob, and Bob sends the value 6 to Alice?

5. There are many variants of the Elgamal signature scheme. Consider a variant where the signature on a message m is a pair (r, s) where

$$\begin{aligned} r &= g^k \bmod p \\ s &= (km + xr) \bmod (p-1) \end{aligned}$$

for a random k. The verification equation checks whether

$$g^s = y^r r^m \bmod p.$$

(a) Show that the verification equation always holds for a valid signature.

(b) Show that if a signer uses the same k value to sign many different messages, then an attacker can forge a signature on any message of its choice.

6. Consider the following two ciphersuite specifications for TLS:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA.

(a) Briefly explain the methods used for key establishment with each of these ciphersuites. Which one of these provides forward secrecy?

(b) How do the two ciphersuites differ in the way that they protect confidentiality and integrity of application data? Compare the security level of the algorithms used for this purpose.

TTM4135 Examination 2018-06-04
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) □