NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758

Examination date: 2015-05-20

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: 1

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 20 questions each worth 1 point.

  Answer the multiple choice problems using the separate answer page. 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 mark.

  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 0.25 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 8 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 encryption algorithms has the largest number of possible keys?

   (a) DES (the Data Encryption Standard algorithm)
   (b) The random simple substitution cipher on an alphabet of 26 characters
   (c) A transposition cipher on blocks of size 10
   (d) The Vigenére cipher with a key of length 5 and an alphabet of 26 characters

2. Following Kerckhoff's principle, we usually assume that an attacker of an encryption scheme has access to:

   (a) unbounded computational power
   (b) the encryption and decryption keys
   (c) the description of the encryption and decryption algorithms
   (d) all of the above.

3. Double encryption with DES (double DES) with two independent keys:

   (a) has twice as many possible key values as ordinary DES
   (b) uses half as much computation as ordinary DES
   (c) runs twice as fast as ordinary DES
   (d) is vulnerable to a meet-in-the-middle attack

4. The AES (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

5. The inverse of 3 modulo 17 is:

   (a) 4
   (b) 1
   (c) 3
   (d) 6

6. Which of the following modes of operation for block ciphers does *not* introduce randomness?

   (a) CBC mode
   (b) CTR mode
   (c) ECB mode
   (d) OFB mode

7. A message authentication code (MAC) provides the security service:

   (a) availability
   (b) non-repudiation
   (c) confidentiality
   (d) data integrity

8. Which of the following is not a binary synchronous stream cipher?

   (a) the one-time pad
   (b) RC4
   (c) SHA-1
   (d) A5/1

9. For numbers of a similar size, and for currently known algorithms:

   (a) factorising numbers is harder than finding prime numbers
   (b) finding prime numbers is harder than factorising numbers
   (c) finding prime numbers and factorising numbers are about the same difficulty
   (d) the best factorisation and prime generation methods use the same algorithm

10. The Fermat test and the Miller–Rabin test are two tests for deciding whether or not a number is prime. Which of the following statements is true?

    (a) The Miller–Rabin test is more reliable than the Fermat test
    (b) The Fermat test is more reliable than the Miller–Rabin test
    (c) The Fermat test and the Miller–Rabin test always give the same result
    (d) The Fermat test and the Miller–Rabin test always give opposite results

11. The keys for the RSA encryption algorithm include a public exponent e, a private exponent d, and a public modulus n. It is common to choose:

    (a) $d = 2^{16} + 1$
    (b) $e = 2^{16} + 1$
    (c) $e = n - 1$
    (d) $d = n - 1$

12. The Diffie-Hellman protocol can be broken by an attacker who is able to:

    (a) solve the discrete logarithm problem
    (b) generate large prime numbers
    (c) perform fast exponentiation
    (d) observe previous runs of the protocol

13. If a hash function outputs random values of length 200 bits then a collision can be expected to occur after:

    (a) 2^{199} elements have been hashed
    (b) 2^{20} elements have been hashed
    (c) 2^{25} elements have been hashed
    (d) 2^{100} elements have been hashed

14. A construction for a message authentication code from any hash function, often used in TLS, is known as:

    (a) CMAC
    (b) HMAC
    (c) SHA-1
    (d) GCM

15. When public key cryptography is used to provide digital signatures:

    (a) the public key of the signer is required in order to verify the signature
    (b) the public key of the verifier is required in order to verify the signature
    (c) the private key of the signer is required in order to verify the signature
    (d) the private key of the verifier is required in order to verify the signature

16. In order to produce a digital certificate, a certification authority computes:

    (a) an encryption of the subject's private key and identity
    (b) an encryption of the subject's public key and identity
    (c) a signature on the subject's private key and identity
    (d) a signature on the subject's public key and identity

17. Forward secrecy is the property that:

    (a) if a user's long term key becomes known to an attacker, session keys established earlier are not compromised
    (b) if a user's long term key becomes known to an attacker, session keys established later are not compromised
    (c) if a user's session key becomes known to an attacker, that user's long term key is not compromised
    (d) if a user's session key becomes known to an attacker, that user's long term key is also compromised

18. Which of these statements about compression in the TLS record protocol is true?

    (a) Compression of payload is essential to provide extra security
    (b) Compression of payload can result in known attacks
    (c) Compression is only applied to headers, not to payload
    (d) Compression is mandatory in all versions of TLS

19. How is the *ciphersuite* used in a run of the TLS protocol decided?

    (a) It is chosen by the server
    (b) It is chosen by the client
    (c) It is negotiated between client and server
    (d) It is defined by the latest version of TLS

20. Which of these TLS ciphersuites provides forward secrecy?

    (a) TLS_RSA_WITH_RC4_128_MD5
    (b) TLS_RSA_WITH_AES_128_CBC_SHA
    (c) TLS_DH_RSA_WITH_AES_128_CBC_SHA256
    (d) TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Exercise 2 Written answer questions

1. One common way of designing modern block ciphers is the *substitution-permutation network*. Each round of such a cipher has three steps: a substitution, a permutation, and a step involving the round key. Explain briefly the operation of each of these steps on the current block state.

2. One mode of operation for block ciphers is counter mode (CTR). The general equation for computing each output block is:

$$C_t = O_t \oplus P_t$$

where $O_t = E(T_t, K)$ and $T_t = N \| t$ is the concatenation of a nonce N and block number t.

Suppose that for a certain faulty implementation the nonce N is always fixed for every message. Explain how an attacker can successfully attack this implementation using a known plaintext attack.

3. In the RSA encryption algorithm the public key is a modulus n and public exponent e where $n = pq$ is the product of two large prime numbers. The private key is the exponent d.

   (a) Show how an attacker who can factorise the modulus n can break the encryption algorithm.

   (b) What are reasonable choices today for the size of n which are both secure and reasonably efficient? How will this change if full-scale quantum computers become available?

4. The Elgamal signature on a message m is a triple (m, r, s) where

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

for a random k such that $\gcd(k, p-1) = 1$. Here $y = g^x \bmod p$ is the public key corresponding to the private key x. The corresponding verification equation is

$$g^m \overset{?}{=} r^s y^r \bmod p.$$

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

   (b) Show that if a signer uses the same random k value to sign two different messages, then the signer's private key can be found.

5. Fermat's theorem states that $a^{p-1} \bmod p = 1$ when p is a prime and $\gcd(a, n) = 1$.

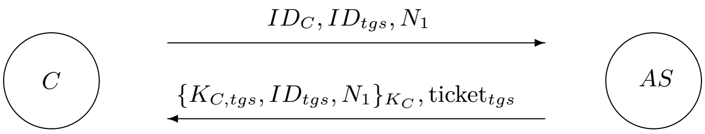
   (a) Illustrate the theorem using one example with respect to the prime $p = 23$.

   (b) Fermat's theorem can be used as the basis of a test to distinguish prime numbers from composite numbers. Explain the basic operation of such an algorithm and illustrate its use for the non-prime $n = 15$.

6. (a) Explain the main similarities and differences between a message authentication code (MAC) and a hash function.

   (b) Why does using the hash of a message instead of a MAC tag fail to provide the properties of a secure MAC?

7. The following message exchange shows a simplified version of the messages exchanged between the client (C) and the authentication server (AS) in the Kerberos protocol.



where $\mathrm{ticket}_{tgs} = \{K_{C,tgs}, ID_C, T_1\}_{K_{tgs}}$ for some validity period T_1.

(a) What is the purpose of the nonce N_1 in this message exchange? How is it used?

(b) Why does the identity ID_{tgs} need to be included in the response message? What could happen if it were omitted?

8. Consider the following ciphersuite specification for TLS:

TLS_RSA_WITH_AES_128_CBC_SHA256

Explain the meaning of each of the elements in the specification, including an indication of which parts are relevant for the Handshake Protocol and which parts are relevant for the Record Protocol.

TTM4135 Examination 2015-05-20
Answer page for Exercise 1 Multiple Choice Questions

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) ☑

NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758/98065197

Examination date: 2015-08-03

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: 1

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 20 questions each worth 1 point.

  Answer the multiple choice problems using the separate answer page. 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 mark.

  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 0.25 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 8 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. A symmetric key cipher must be secure against brute-force key search. A reasonable *minimum* key length for industry-standard security today is:

   (a) 32 bits
   (b) 128 bits
   (c) 512 bits
   (d) 1024 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 encryption and decryption keys
   (c) the description of the encryption and decryption algorithms
   (d) all of the above.

3. Triple encryption with DES (triple DES) with three independent keys:

   (a) uses three times as much computation as ordinary DES
   (b) has three times as many possible key values as ordinary DES
   (c) runs three times faster than ordinary DES
   (d) is vulnerable to brute-force key search today

4. The AES (Advanced Encryption Standard) algorithm:

   (a) is based on a Feistel cipher design
   (b) is based on a substitution-permutation network (SPN) design
   (c) was replaced by the Data Encryption Standard (DES) cipher
   (d) was replaced by the Digital Signature Standard (DSS)

5. The inverse of 4 modulo 19 is:

   (a) 1
   (b) 5
   (c) 10
   (d) 15

6. A mode of operation for a block cipher often introduces a random IV. This is useful for security because:

   (a) it adds to the complexity of decryption
   (b) it increases the difficulty of brute-force key search
   (c) the same ciphertext is decrypted to different messages
   (d) the same plaintext is encrypted to different ciphertexts

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

8. The one-time pad achieves perfect secrecy. This means that:

   (a) each plaintext is a perfectly random string
   (b) the only feasible attack is brute-force key search
   (c) an attacker cannot alter any bit in the ciphertext without this being detected
   (d) an attacker learns nothing about the plaintext from the ciphertext

9. For numbers of 2048 bits in size there are known efficient algorithms which can be implemented for:

   (a) factorising numbers
   (b) taking discrete logarithms
   (c) generating random prime numbers
   (d) performing exhaustive key search

10. 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

11. The RSA encryption algorithm uses a public modulus n. Regarding the security of the RSA algorithm it is known that:

    (a) a known plaintext attack allows an attacker to obtain the private key
    (b) finding the plaintext from any ciphertext is as hard as finding the factors of n
    (c) finding the private key from the public key is as hard as finding the factors of n
    (d) quantum computers would not help in an attack

12. The Elgamal encryption algorithm can be broken by an attacker who is able to:

    (a) solve the discrete logarithm problem
    (b) generate large prime numbers
    (c) perform fast exponentiation
    (d) perform a chosen ciphertext attack

13. 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

14. HMAC is a construction for a message authentication code, often used in TLS. The HMAC algorithm:

    (a) is vulnerable to length extension attacks

    (b) has output size equal to the input size

    (c) uses a single call to the underlying hash function

    (d) can use any iterated hash function

15. When public key cryptography is used to provide digital signatures:

    (a) the public key of the signer is required in order to generate the signature

    (b) the public key of the verifier is required in order to generate the signature

    (c) the private key of the signer is required in order to generate the signature

    (d) the private key of the verifier is required in order to generate the signature

16. A digital certificate is issued by a certification authority. It must include:

    (a) the subject's private key and identity

    (b) the subject's public key and identity

    (c) the certificate authority's private key

    (d) a certificate revocation list

17. In the Kerberos system three kinds of server are involved. A ticket granting ticket (TGT) may be issued by:

    (a) authentication server

    (b) ticket-granting server

    (c) application server

    (d) any type of server

18. Which of the following is *not* explicitly negotiated during the TLS handshake protocol?

    (a) The version of TLS to be used

    (b) The algorithms to be used for exchange of the session key

    (c) The encryption algorithm to be used in the record protocol

    (d) The security services to be provided by the record protocol

19. The TLS sub-protocol concerned with providing confidentiality and integrity to application data is called:

    (a) the handshake protocol

    (b) the record protocol

    (c) the alert protocol

    (d) the change cipher spec protocol

20. One commonly used TLS ciphersuite is denoted as TLS_RSA_WITH_AES_128_CBC_SHA. When this ciphersuite is chosen, RSA is used:

    (a) to sign the server ephemeral Diffie-Hellman value

    (b) to sign the client ephemeral Diffie-Hellman value

    (c) to encrypt the pre-master secret with the server long-term key

    (d) to encrypt the pre-master secret with the client long-term key

Exercise 2 Written answer questions

1. One common way of designing modern block ciphers is to use the Feistel construction. The equations for round i are usually written as follows.

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   (a) Describe what is represented by the values L_i, R_i and K_i in the above equations.

   (b) Write down the corresponding equations used to compute L_{i-1} and R_{i-1}, given L_i and R_i, during decryption.

   (c) Why is it *not* necessary for the function f to be invertible in order to be able to decrypt?

2. One mode of operation for block ciphers is cipher block chaining (CBC). CBC mode can be used either to encrypt the sequence of blocks $P_1, P_2, \ldots, P_n$ or to form a message authentication code (MAC) from the last ciphertext block. The general equation for computing each ciphertext block, where C_0 = IV, is:

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

   (a) Suppose first that CBC mode is used for encryption but IV is chosen to be the same for every message. Explain why this is a weakness and how it might be used by an attacker.

   (b) Suppose now that CBC mode is used to form a MAC and now the IV is chosen randomly for each message and sent with the MAC. Explain how an attacker can forge a valid MAC for any one-block message, given a valid MAC on any other one-block message.

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 $d = 27$ and the ciphertext is $C = 2$. Specifically, compute M_p and M_q and apply the CRT to find M.

4. In public key cryptography it is often required to compute values of the form $a^b \bmod n$ for some randomly chosen exponent b and large modulus n. This is often achieved using the *square-and-multiply* method.

   (a) Without using any specific values for a or n, illustrate how the square-and-multiply method works by showing the steps required to compute $a^{37} \bmod n$. How many squarings and how many multiplications are needed?

   (b) If n and b are 2000 bits in length, what is the expected number of squarings and multiplications needed to apply the *square-and-multiply* method? How does this vary with different values of b?

5. The Elgamal encryption scheme works in $\mathbb{Z}_p^*$ for a prime p. The public key is $y = g^x \bmod p$ and the private key is the exponent x. To encrypt a message m the ciphertext is the pair $c = (g^k \bmod p, my^k \bmod p)$.

   (a) Explain how an attacker who can take discrete logarithms can find the message from the ciphertext and public key.

   (b) What are reasonable choices today for the size of p which are both secure and reasonably efficient? How will this change if full-scale quantum computers become available?

6. When using the RSA algorithm to form a digital signature, the output is a value $s = h(m)^d \bmod n$ for a suitable hash function h. The message m and s are sent to the verifier.

   (a) Given a valid public exponent e, how does the verifier check the signature?

   (b) Explain how an attacker who can find a *collision* in h can exploit this to construct a message forgery.

7. Consider the following protocol with the goal of key establishment. Here N_A is a nonce chosen by A, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

   1. $A \to B : ID_A, N_A$
   2. $B \to S : ID_A, ID_B, N_A$
   3. $S \to B : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{AS}}, \{K_{AB}, ID_A, ID_B, N_A\}_{K_{BS}}$
   4. $B \to A : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{AS}}$

   Describe a replay attack on this protocol, showing concrete messages sent by the attacker.

8. Consider the protocol below as an abstract version of the TLS handshake protocol. Client C and server S have negotiated a ciphersuite incorporating ephemeral Diffie-Hellman. The Diffie-Hellman group generator is g and the server certificate is $Cert_S$. The server and client choose random values x and y respectively and the server uses a signature scheme denoted Sig_S.

$$\begin{aligned} S \to C\text{:} &\quad Cert_S, g^x, Sig_S(g^x) \\ C \to S\text{:} &\quad g^y \end{aligned}$$

   (a) Explain how both C and S will compute the TLS session keys.

   (b) Explain why this protocol achieves forward secrecy.

Detach this sheet and hand it in together with your written answers

TTM4135 Examination 2015-08-03
Answer page for Exercise 1 Multiple Choice Questions

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) □

NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758

Examination date: 2016-05-28

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: 1

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 25 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 7 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. If a plaintext comes from a natural language, such as English, which of the following encryption algorithms can be expected to have a more even (“flatter”) frequency distribution of ciphertext characters?

   (a) The Caesar cipher
   (b) The random simple substitution cipher
   (c) A transposition cipher on blocks of size 10
   (d) The Vigenére cipher with a key of length 5

2. Which of the following is a fundamental weakness of the Hill cipher for *any* size of encryption matrix?

   (a) The number of possible keys is too small
   (b) Encryption is a linear function
   (c) The encryption function is computationally expensive
   (d) Decryption is not always possible

3. 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.

4. In an iterative block cipher the purpose of the *key schedule* is to:

   (a) define how to derive the round keys from the master key;
   (b) generate different keys for every block encrypted;
   (c) choose between different master keys;
   (d) define how the master key is generated.

5. For any given values x and m, the square-and-multiply algorithm when used to compute $x^{66} \bmod m$ requires:

   (a) 5 squarings and 3 multiplication modulo m
   (b) 6 squarings and 1 multiplication modulo m
   (c) 8 squarings and 1 multiplication modulo m
   (d) 63 squarings and 1 multiplication modulo m

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

   (a) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 11$
   (b) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 11$
   (c) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 12$
   (d) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 12$

7. Let g be a generator for the integers modulo p. The discrete logarithm problem is:

   (a) given y, find x with $y = x^g \bmod p$;
   (b) given x, find y with $y = x^g \bmod p$.
   (c) given y, find x with $y = g^x \bmod p$;
   (d) given x, find y with $y = g^x \bmod p$.

8. Which of the following block cipher modes of operation is *not* designed to provide data confidentiality?

   (a) Counter mode (CTR)
   (b) Cipher block chaining (CBC)
   (c) Cipher-based MAC (CMAC)
   (d) Counter with CBC-MAC (CCM)

9. The main disadvantage of basic Electronic Code Book (ECB) mode of operation for block ciphers, in comparison with counter mode (CTR) and cipher block chaining (CBC) mode, is:

   (a) ECB mode encryption is less efficient;
   (b) ECB mode has large error propagation;
   (c) equal plaintext blocks in ECB mode give equal ciphertext blocks;
   (d) ECB mode requires longer keys.

10. Which of these statements about the keystream used in the one time pad is *false*?

    (a) The keystream is completely random
    (b) The keystream is as long as the message
    (c) The keystream is generated by a linear feedback shift register (LFSR)
    (d) The keystream is only used once

11. The maximum period of a linear feedback shift register with 10 binary storage locations is:

    (a) 10
    (b) 512
    (c) 1023
    (d) 1024

12. In the RSA encryption algorithm it is common to use the Chinese Remainder Theorem to:

    (a) speed up the encryption process;
    (b) speed up the decryption process;
    (c) speed up the key generation process;
    (d) all of the above.

13. The RSA encryption scheme uses a public exponent e, a private exponent d, and a public modulus n which is the product of two primes p and q. Regarding security of the scheme it is known that:

    (a) knowledge of n and e is sufficient to find d;

    (b) an attacker who can encrypt a random message can find d;

    (c) finding d from p and q is as hard as factorising n;

    (d) an attacker who can find d is able to also find p and q

14. ElGamal encryption in $\mathbb{Z}_p^*$ uses a modulus p, while RSA encryption uses a composite modulus n. When these are chosen to be of the same length:

    (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.

15. Three important computational problems in cryptography are: the discrete logarithm problem in $\mathbb{Z}_p^*$ (DLP), the discrete logarithm problem in elliptic curves (ECDLP) and the integer factorisation (IF) problem. If full-scale quantum computers become available then we know that:

    (a) all three of these problems will have efficient solutions;

    (b) only IF will have an efficient solution;

    (c) only DLP will have an efficient solution;

    (d) only IF and DLP will have efficient solutions.

16. HMAC is an algorithm often used in TLS. It is based on any iterated hash function. Which of these statements with regard to HMAC is *false*?

    (a) HMAC takes a shared secret key as one input;

    (b) the output size of HMAC is the same as the output size of the hash function;

    (c) the message input to HMAC is of variable length;

    (d) both the hash function and HMAC provide message integrity.

17. Galois counter mode (GCM) is often used in TLS to provide:

    (a) data confidentiality;

    (b) data integrity;

    (c) error checking;

    (d) authenticated encryption.

18. When public key cryptography is used to provide digital signatures:

    (a) the public key of the signer is required in order to generate the signature;

    (b) the public key of the verifier is required in order to generate the signature;

    (c) the private key of the signer is required in order to generate the signature;

    (d) the private key of the verifier is required in order to generate the signature.

19. The Digital Signature Algorithm (DSA) is a standardised algorithm based on ElGamal signatures. Compared with RSA signatures at the same security level which of the following is true?

    (a) DSA signatures are shorter than RSA signatures;

    (b) DSA signatures are more efficient to verify, even if the public RSA exponent equals 3;

    (c) DSA signatures cannot use elliptic curve groups but RSA signatures can;

    (d) DSA signatures do not require a random input but RSA signatures do.

20. If we choose elements randomly from a set of 1 000 000 values then, according to the birthday paradox, a collision will occur with probability 0.5 after approximately:

    (a) 999 999 elements have been chosen;

    (b) 500 000 elements have been chosen;

    (c) 1 000 elements have been chosen;

    (d) 20 elements have been chosen.

21. When assessing the security of a key establishment protocol such as the Needham–Schroeder protocol, we assume that an attacker is able to:

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

    (b) obtain the long-term key of the parties involved in the protocol run under attack;

    (c) break any encryption algorithm used in the protocol;

    (d) force any protocol participant to repeat nonce values.

22. Forward secrecy is provided in TLS as long as the handshake protocol uses:

    (a) ephemeral Diffie-Hellman;

    (b) static Diffie-Hellman;

    (c) RSA with a 1024 bit modulus;

    (d) RSA with a 2048 bit modulus.

23. TLS consists of a number of protocols. The protocol responsible for providing confidentiality and data integrity to payload data is called:

    (a) the handshake protocol;

    (b) the record protocol;

    (c) the alert protocol;

    (d) the change cipher spec protocol.

24. A difference between the public key infrastructure used by TLS for web browsers, and that provided by PGP for email security, is:

    (a) PGP keys can be signed by any other user;

    (b) PGP keys are certified in a hierarchical manner;

    (c) PGP keys have no expiry date;

    (d) PGP keys can use any type of public key algorithm.

25. Like TLS, IPSec can be used to set up secure communication between nodes. Which of the following applies to IPSec, but *not* to TLS?

    (a) Different suites of cryptographic algorithms can be used.

    (b) Traffic flow confidentiality may be provided.

    (c) Forward secrecy may be provided using Diffie-Hellman key exchange.

    (d) The protocol specification defines *both* key establishment and security of user data.

Exercise 2 Written answer questions

1. Suppose that a certain encryption algorithm uses a secret key of 64 bits and that an attacker has the ability to test all possible keys within one year.

   (a) Estimate how many keys per second the attacker can test. (You may use the approximation that there are 2^{25} seconds in a year.)

   (b) Given a particular ciphertext to test, how could this attacker know when the correct key is found?

   (c) If the key length is increased to 72 bits, how long will it take the attacker to test all keys if the rate of testing is the same? In practice, would you expect the rate of testing to stay constant in this time period? 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.

   Suppose that a message of 4 blocks, P_1, P_2, P_3, P_4 is encrypted using CBC mode into a ciphertext with 4 blocks, C_1, C_2, C_3, C_4. Using either the encryption/decryption equations, or an appropriate diagram, explain what happens in the following independent experiments.

   (a) If one bit is flipped in message block P_2 and the whole message is re-encrypted, how different are the new ciphertext blocks C'_1, C'_2, C'_3, C'_4 in comparison with the original ciphertext blocks C_1, C_2, C_3, C_4?

   (b) If one bit is flipped in ciphertext block C_2 and the whole message is decrypted, how different are the new decrypted plaintext blocks P'_1, P'_2, P'_3, P'_4 in comparison with the original plaintext blocks P_1, P_2, P_3, P_4?

3. 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 that 3 *is* a generator.

   (b) Consider Diffie–Hellman key exchange in $\mathbb{Z}_p^*$ when $p = 17$ and $g = 3$. If principal A chooses random secret input value $a = 3$ and receives message $y = 8$ from B, what is the shared secret which they both obtain?

4. An RSA signature on a message m is a pair (m, s) where $s = h(m)^d \bmod n$, h is a suitable hash function, and n is the modulus which is part of the public key (e, n).

   (a) Given an RSA signature (m, s), explain how a recipient should verify the signature.

   (b) Suppose that an attacker can obtain valid signatures for messages of the attacker's choice, known as a *chosen message attack*. What property is required of the hash function h in order to prevent such an attacker from finding an existential forgery?

   (c) Suppose that h is chosen to be the function $h(m) = m + 1 \bmod n$. Describe how an existential forgery can be found by an attacker without access to any other valid signature.

5. (a) Explain the main similarities and differences between a message authentication code (MAC) and a digital signature.

   (b) In the TLS protocol between a client and a server it is common to use MACs and digital signatures. Describe one part of the TLS protocol where a MAC is used and one part where a signature is used. Could the same choice (MAC or signature) be used in *both* places?

6. Consider the following protocol with the goal of key establishment. Here N_A is a nonce chosen by A, N_B is a nonce chosen by B, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

   1. $A \rightarrow S : ID_A, ID_B, N_A$
   2. $S \rightarrow A : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{AS}}$
   3. $S \rightarrow B : \{K_{AB}, ID_A, ID_B, N_A\}_{K_{BS}}$
   4. $B \rightarrow A : \{ID_B, ID_A, N_A, N_B\}_{K_{AB}}$
   5. $A \rightarrow B : \{ID_A, ID_B, N_A, N_B\}_{K_{AB}}$

   Describe a replay attack on this protocol, showing concrete messages sent by the attacker.

7. 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) Why is there a fundamental problem in providing forward secrecy for electronic mail (email)?

TTM4135 Examination 2016-05-28
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) □

NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Telematics

Examination paper for TTM4135 Information security

Academic contact during examination: Colin Boyd

Phone: 73551758

Examination date: 2016-08-18

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: 1

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 25 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 7 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. Cryptanalysis of the Vigenére cipher often uses autocorrelation in order to:

   (a) identify the period (key length)
   (b) determine the shift for a specific substitution alphabet
   (c) check if the original plaintext message is periodic
   (d) predict the likely plaintext

2. When assessing the security of an iterative block cipher, which of the following do we usually assume is *not* available to the attacker?

   (a) The ciphertext under attack
   (b) A small amount of ciphertext and corresponding plaintext
   (c) The round keys
   (d) The specification of the encryption algorithm

3. 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

4. In a block cipher designed as a substitution-permutation network the purpose of an *S-box* is to:

   (a) substitute sub-blocks by other sub-blocks
   (b) permute different bit positions in the whole block
   (c) substitute plaintext bits by key bits
   (d) derive round keys from the master key

5. For any given values x and m, the square-and-multiply algorithm when used to compute $x^{36} \bmod m$ requires:

   (a) 5 squarings and 1 multiplication modulo m
   (b) 6 squarings and 2 multiplications modulo m
   (c) 5 squarings and 3 multiplications modulo m
   (d) 6 squarings and 4 multiplications modulo m

6. The Chinese Remainder Theorem is often used to solve simultaneous equations of the form $x \equiv c_1 \bmod d_1$ and $x \equiv c_2 \bmod d_2$. A solution can always be found if:

   (a) $c_1 \neq c_2$
   (b) $d_1 \neq d_2$
   (c) $\gcd(c_1, c_2) = 1$
   (d) $\gcd(d_1, d_2) = 1$

7. Let $g = 2$ be a generator for the integers modulo 11. The discrete logarithm of 5 is then:

   (a) 3
   (b) 4
   (c) 5
   (d) 6

8. Which of the following block cipher modes of operation has a fixed length output, independent of the message length?

   (a) Counter mode (CTR)
   (b) Cipher block chaining (CBC)
   (c) Cipher-based MAC (CMAC)
   (d) Counter with CBC-MAC (CCM)

9. Two modes of operation for block ciphers are counter mode (CTR) and cipher block chaining (CBC) mode. One property held by CTR mode and *not* held by CBC mode is:

   (a) encryption includes a random input
   (b) decryption in the mode uses *encryption* for the basic block cipher
   (c) equal plaintext blocks always encrypt to equal ciphertext blocks
   (d) authentication is provided

10. Two binary additive stream ciphers are the AES block cipher in counter (CTR) mode, and the (binary) one time pad. An advantage of using AES in CTR mode is:

   (a) the error propagation properties are better
   (b) the level of confidentiality is higher
   (c) the key management process is more efficient
   (d) the encryption algorithm is simpler

11. Suppose a linear feedback shift register (LFSR) with 40 binary storage locations is used as a keystream generator for a binary additive stream cipher. The main weakness of this cipher is:

   (a) the period of the keystream cannot be greater than 80
   (b) a known plaintext attack is easy given 80 bits of plaintext/ciphertext
   (c) if the key defines the position of the feedback taps then there are at most 80 keys
   (d) if the key defines the initial LFSR state then there are at most 80 keys

12. The Fermat test for whether or not a number n is prime is based on which of the following, when $\gcd(a, n) = 1$?

   (a) If $a^{n-1} \bmod n = 1$ then n must be prime
   (b) If $a^{n-1} \bmod n = 1$ then n must be composite
   (c) If n is composite then $a^{n-1} \bmod n = 1$
   (d) If n is prime then $a^{n-1} \bmod n = 1$

13. 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) $ed \equiv 1 \bmod n$

    (b) $ed \equiv \phi(n) \bmod n$

    (c) $ed \equiv 1 \bmod \phi(n)$

    (d) $ed \equiv n - 1 \bmod \phi(n)$

14. When using an RSA public key today for a secure TLS connection, a reasonable minimum choice of modulus length is:

    (a) 128 bits

    (b) 512 bits

    (c) 2048 bits

    (d) 4096 bits

15. 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^{255} trials

16. Forward secrecy is the property that:

    (a) if a user's long term key becomes known to an attacker, session keys established earlier are not compromised

    (b) if a user's long term key becomes known to an attacker, session keys established later are not compromised

    (c) if a user's session key becomes known to an attacker, that user's long term key is not compromised

    (d) if a user's session key becomes known to an attacker, that user's long term key is also compromised

17. The TLS protocol typically provides both confidentiality and data integrity for user data. Which of the following is *not* suitable to provide both of these services?

    (a) AES in GCM mode

    (b) AES in CBC mode with HMAC

    (c) AES in CCM mode

    (d) AES in CTR mode

18. When public key cryptography is used to provide digital signatures:

    (a) the public key of the signer is required in order to verify the signature

    (b) the public key of the verifier is required in order to verify the signature

    (c) the private key of the signer is required in order to verify the signature

    (d) the private key of the verifier is required in order to verify the signature

19. 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

20. 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

21. When assessing the security of a key establishment protocol, such as the Needham–Schroeder protocol, we assume that an attacker is able to:

    (a) obtain any session keys used in previous runs of the protocol
    (b) obtain the long-term key of the parties involved in the protocol run under attack
    (c) break any encryption algorithm used in the protocol
    (d) force any protocol participant to repeat nonce values

22. RSA signatures are often used for signing digital certificates in preference to using DSA signatures. One reason for this is:

    (a) RSA signatures are shorter with usual parameters
    (b) RSA signatures are faster to verify with usual parameters
    (c) RSA signatures are more secure with the same size public key
    (d) RSA signatures remain secure against quantum computers

23. TLS consists of a number of protocols. The protocol responsible for negotiating the ciphersuite used in a particular TLS instance is called:

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

24. Email does not use an interactive protocol between sender and receiver. As a consequence:

    (a) it is not possible to provide end-to-end security for email
    (b) it is not possible to use public key cryptography in email security
    (c) it is not possible to provide data integrity for email
    (d) it is not possible to provide forward secrecy for email

25. Two modes of usage for IPsec are *tunnel mode* and *transport mode*. A characteristic of tunnel mode, not shared with transport mode is that:

    (a) the original IP header is sent in cleartext (not encrypted)
    (b) a completely new IP header is constructed for each packet
    (c) the original payload data is encrypted
    (d) the original payload data is authenticated

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. Assume that the alphabet has only five letters encoded as $A = 0, B = 1, C = 2, D = 3, E = 4$.

   Suppose that the encryption key for a 2 x 2 Hill cipher is $K = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}$.

   (a) Encrypt the plaintext ABCD.

   (b) Determine the decryption key K^{-1}.

   (c) Decrypt the ciphertext DCBA.

   Give all results using integers in the range 0 to 4 inclusive.

2. One mode of operation for the AES block cipher 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.

   Answer the following questions, with explanation, when CBC mode is applied.

   (a) What is the equation for decryption of ciphertext block C_t?

   (b) Is it possible to encrypt several blocks in parallel?

   (c) Is it possible to decrypt several blocks in parallel?

   (d) If one bit is flipped in one ciphertext block, how many bits are affected in the plaintext after decryption?

3. The Elgamal encryption scheme encrypts a message M to a ciphertext pair $C = (r, s)$ using a random k and public key y as follows.

   $$\begin{aligned} r &= g^k \bmod p \\ s &= My^k \bmod p \end{aligned}$$

   (a) Explain how the owner of the corresponding private key decrypts and obtains the plaintext from C.

   (b) Suppose a faulty implementation uses the same k value every time a message is encrypted. How can an attacker with access to a single plaintext/ciphertext pair use that to decrypt any other ciphertext?

4. 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 $n = 35 = 5 \times 7$, the decryption exponent is $d = 17$ and the ciphertext is $C = 2$. Specifically, compute M_p and M_q and apply the CRT to find M.

5. A message authentication code (MAC) computes a tag T for a message M given key K. Such a MAC is often defined using a cryptographic hash function H such as SHA-256.

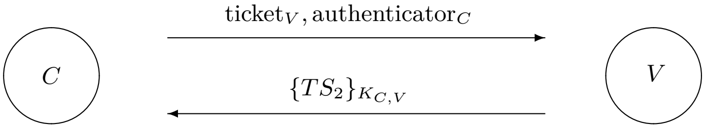
   (a) Explain how a recipient of a message M and a tag T should check the integrity of the received message.

   (b) Consider the weak MAC function which computes the tag T as:

   $$T = H(M) \oplus H(K)$$

   How can an attacker who sees a valid (M, T) pair compute a valid tag on any chosen message M'?

6. The following message exchange shows a simplified version of the messages exchanged between the client (C) and the application server (V) in the Kerberos protocol. (Note this is the *third* interaction in the protocol, following exchanges with the authentication server and ticket granting server.)



   where

   $$\begin{aligned} \mathrm{ticket}_V &= \{K_{C,V}, ID_C, T_2\}_{K_V} \text{ for some validity period } T_2 \\ \mathrm{authenticator}_C &= \{ID_C, TS_2\}_{K_{C,V}} \text{ for some timestamp } TS_2. \end{aligned}$$

   (a) Explain the different purposes of ticket_V and $\mathrm{authenticator}_C$.

   (b) Explain how C can use the second message to authenticate V.

7. Consider the following ciphersuite specification for TLS:

   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

   (a) The letters EC mean that this ciphersuite uses elliptic curves. What is the advantage of using elliptic curves compared with using groups $\mathbb{Z}_p^*$?

   (b) The letters DHE mean that this ciphersuite uses ephemeral Diffie–Hellman values. What is the advantage of this compared with using static Diffie–Hellman values?

   (c) What is the ECDSA signature used for in this ciphersuite?

   (d) How is user data authenticated in this ciphersuite?

TTM4135 Examination 2016-08-18
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) □

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: 2017-05-19

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 integers does *not* have an inverse modulo 21?
   - (a) 1
   - (b) 2
   - (c) 3
   - (d) 4
2. Which of the following integers is a *generator* for $\mathbb{Z}_7^*$, the non-zero integers modulo 7?
   - (a) 1
   - (b) 2
   - (c) 3
   - (d) 6
3. If a plaintext comes from a natural language, such as English, which of the following encryption algorithms can be expected to have the most uniform (“flattest”) frequency distribution of ciphertext characters?
   - (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 of the following key sizes is the smallest which would be acceptable to prevent exhaustive key search today?
   - (a) 32 bits
   - (b) 64 bits
   - (c) 128 bits
   - (d) 256 bits
5. 3-DES is a variant of the original Data Encryption Standard (DES) algorithm. In 3-DES:
   - (a) the original DES algorithm is run three times for each input block
   - (b) the block size is three times longer than original DES
   - (c) the algorithm runs three times faster than original DES
   - (d) there are three times as many possible keys as original DES
6. The Data Encryption Standard (DES) is an iterated block cipher. In each round the DES 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. Which of the following block cipher modes of operation is *not* designed to provide data integrity?

   (a) Galois counter mode (GCM)
   (b) Cipher block chaining (CBC)
   (c) Cipher-based MAC (CMAC)
   (d) Counter with CBC-MAC (CCM)

8. Counter mode (CTR) is a mode of operation for block ciphers. Which of the following statements about CTR mode is true?

   (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. Which of these statements about the keystream used in the one time pad is true?

   (a) The keystream has a large, but finite, period
   (b) The keystream starts with an initialisation vector (IV)
   (c) The keystream is generated by a linear feedback shift register (LFSR)
   (d) Each keystream bit is only used once

10. In a binary synchronous stream cipher:

   (a) the keystreams generated by the sender and receiver are the same
   (b) the keystreams generated by the sender and receiver are complementary (every bit is different)
   (c) the keystream generated by the receiver is the XOR sum of the plaintext and the keystream generated by the sender
   (d) the keystream generated by the receiver is the XOR sum of the ciphertext and the keystream generated by the sender

11. In typical usage, a true random number generator (TRNG) and a pseudo-random number generator (PRNG) are often combined in practice so that:

   (a) the PRNG provides the seed for the TRNG
   (b) the TRNG provides the seed for the PRNG
   (c) the TRNG and the PRNG output alternate bits
   (d) the TRNG and PRNG output is combined using exclusive-OR

12. Consider the pair of equations: $x \equiv c_1 \bmod d_1$ and $x \equiv c_2 \bmod d_2$. These equations can be solved using the Chinese Remainder Theorem as long as:

   (a) $\gcd(c_1, c_2) = 1$
   (b) $\gcd(d_1, d_2) = 1$
   (c) $\gcd(c_1, d_1) = 1$
   (d) $\gcd(c_2, d_2) = 1$

13. The value of the Euler function $\phi(100)$ is:

    (a) 40
    (b) 50
    (c) 60
    (d) 80

14. Many cryptographic systems are based on the integer factorisation problem. Which of the following statements regarding factorisation is true?

    (a) The best known algorithm for integer factorisation runs in exponential time in the length of the input
    (b) The difficulty of integer factorisation is the same as the difficulty of finding prime numbers of the same length
    (c) There is as efficient integer factorisation algorithm using quantum computers
    (d) An integer of 256 bits is too hard to factorise in practice

15. When public key cryptography is used for encryption:

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

16. The RSA encryption scheme uses a public exponent e, a private exponent d, and a public modulus n which is the product of two primes p and q. Regarding security of the scheme it is known that:

    (a) with knowledge of n and e it is easy to find d
    (b) an attacker who can encrypt a random message can find d
    (c) finding d from e and n is no harder than factorising n
    (d) finding d from p, q and e is hard

17. For the RSA encryption scheme a large modulus n is chosen, typically around 2048 bits in practice. To improve efficiency, this is often used together with:

    (a) a small value for e
    (b) a small value for d
    (c) a small value for one of the factors of n
    (d) a small value for the Euler function $\phi(n)$

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

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

19. Consider the group $\mathbb{Z}_{11}^*$ with generator $g = 2$. If $y = 5$ then the discrete logarithm of y, is
    (a) 2
    (b) 3
    (c) 4
    (d) 5

20. 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

21. HMAC is an algorithm often used in TLS and based on a hash function H. Which of these statements with regard to HMAC is true?
    (a) HMAC does not use a secret key
    (b) The output size of HMAC varies with the size of the input message
    (c) The message input to HMAC must be of a fixed length
    (d) The hash function H can be any iterated hash function

22. ECDSA is a standardised algorithm for digital signatures using elliptic curve groups. Which of the following statements about ECDSA is true?
    (a) The ECDSA algorithm is believed to be secure against quantum computers
    (b) ECDSA has shorter public keys than those for DSA signatures in $\mathbb{Z}_p^*$, for the same security level
    (c) ECDSA signatures are larger than RSA signatures, for the same security level
    (d) It is required that a different elliptic curve is generated for each user of ECDSA

23. An X.509 digital certificate is issued by a certification authority. It must include:
    (a) the subject's private key and identity
    (b) the subject's public key and identity
    (c) the certificate authority's private key
    (d) a digital signature signed by the subject

24. 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

25. The original Needham–Schroeder protocol is known to be vulnerable to a replay attack. This means that:

    (a) an honest party accepts a session key used in a previous run of the protocol
    (b) an honest party re-uses its nonce used in a previous run of the protocol
    (c) the attacker obtains the long-term key of an honest party
    (d) the attacker obtains the nonce used by an honest party

26. The purpose of the *record 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 messages

27. One commonly used TLS ciphersuite is denoted as TLS_RSA_WITH_AES_128_GCM_SHA256. When this ciphersuite is chosen, RSA is used:

    (a) to sign the server certificate
    (b) to sign the client certificate
    (c) to encrypt the pre-master secret with the server long-term key
    (d) to encrypt the pre-master secret with the client long-term key

28. When TLS uses authenticated encryption modes, such as CCM or GCM, the additional authenticated data includes:

    (a) the session key
    (b) the pre-master secret
    (c) the peer certificate
    (d) the sequence number and header data

29. Two alternative methods of providing assurance in the correctness of public keys are a *web of trust* and a *hierarchical infrastructure*. An important difference between the two is:

    (a) which set of entities is able to sign public keys
    (b) the way that private keys are kept confidential
    (c) the length of time for which the public keys remain valid
    (d) the signature algorithms used

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 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 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. One mode of operation for block ciphers is counter mode (CTR). The general equation for computing each output block is:

   $$C_t = O_t \oplus P_t$$

   where $O_t = E(T_t, K)$ and $T_t = N \| t$ is the concatenation of a nonce N and block number t.

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

   (b) If one bit is flipped in ciphertext block C_t, how many bits are changed in the decrypted plaintext? Explain your answer.

   (c) Define a message authentication code (MAC) so that the last complete block of the message encrypted with CTR is the MAC tag. Would this be a good MAC? Explain your answer.

2. Public key cryptosystems are often implemented in a group of non-zero elements in a group formed by multiplication with respect to some modulus.

   (a) For the case $\mathbb{Z}_p^*$ for a prime number p, every element has an inverse. What does it mean to be the inverse of an element x?

   (b) What is the inverse of 3 when $p = 13$?

   (c) When n is composite, the structure of $\mathbb{Z}_n^*$ is different. What are the elements of $\mathbb{Z}_{15}^*$?

3. In public key cryptography it is often required to compute values of the form $a^b \bmod n$ for some randomly chosen exponent b and large modulus n. This is often achieved using the *square-and-multiply* method.

   (a) Without using any specific values for a or n, illustrate how the square-and-multiply method works by showing the steps required to compute $a^{71} \bmod n$. How many squarings and how many multiplications are needed?

   (b) If n and b are 2400 bits in length, what is the expected number of squarings and multiplications needed to apply the square-and-multiply method?

4. Consider a weak variant of the RSA signature on a message m. The signed message is a pair (m, s) where $s = h(m)^d \bmod n$, h is a hash function, and n is the modulus which is part of the public key (e, n). Unlike the normal RSA signature, the values d and e are related using the equation

   $$d = -e \bmod \phi(n).$$

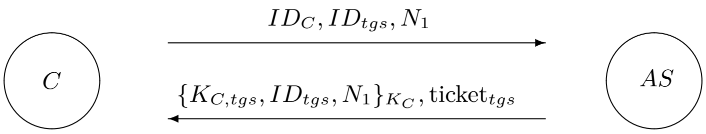
   (a) The verification equation for a received signature (m, s) is to check that

   $$s \times h(m)^e \bmod n = 1.$$

   Explain why a valid signature will always satisfy the verification equation, as long as $\gcd(h(m), n)) = 1$.

   (b) Explain why it is easy for an attacker to forge a valid signature on any message m.

5. The following message exchange shows a simplified version of the messages exchanged between the client (C) and the authentication server (AS) in the Kerberos protocol.



   where $\text{ticket}_{tgs} = \{K_{C,tgs}, ID_C, T_1\}_{K_{tgs}}$ for some validity period T_1.

   (a) What is the purpose of the nonce N_1 in this message exchange? How is it processed by each party?

   (b) Why is the identity ID_C included in ticket_{tgs}? What attack could happen if this identity field is not included in the ticket?

6. Two different protocols often used to protect email in transit are PGP and STARTTLS.

   (a) To what extent do these protocols protect email from a malicious email server?

   (b) How do each of these protocols affect processing requirements for email servers and email clients?

TTM4135 Examination 2017-05-19
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) □

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: 2017-08-08

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 integers is a square root of 1 modulo 21?

   (a) 2
   (b) 4
   (c) 6
   (d) 8

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

3. For which one of the following encryption algorithms are the distributions of plaintext and ciphertext characters the same?

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

4. Which of the following is *not* a valid key size for the AES cipher?

   (a) 128 bit
   (b) 192 bits
   (c) 256 bits
   (d) 512 bits

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. Which of the following block cipher modes of operation is *not* designed to provide data confidentiality?

   (a) Galois counter mode (GCM)
   (b) Cipher block chaining (CBC)
   (c) Cipher-based MAC (CMAC)
   (d) Counter with CBC-MAC (CCM)

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

   (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 single bit in error in the decrypted plaintext
   (c) Equal plaintext blocks encrypt to equal ciphertext blocks
   (d) Encryption of a sequence of blocks can be conducted in parallel

9. The one-time pad achieves perfect secrecy. This means that:

   (a) each plaintext message is a perfectly random string
   (b) the only feasible attack is brute-force key search
   (c) an attacker cannot alter any bit in the ciphertext without this being detected
   (d) an attacker learns nothing about the plaintext from the ciphertext

10. When using counter mode encryption with a block cipher, a binary keystream is generated by the sender. The keystream generated by the recipient is:

    (a) the same as that generated by the sender
    (b) the complement of that generated by the sender (every bit is different)
    (c) random and independent of that generated by the sender
    (d) random but dependent on the ciphertext received

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

    (a) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 17$
    (b) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 17$
    (c) $x \equiv 3 \bmod 5$ and $x \equiv 3 \bmod 18$
    (d) $x \equiv 3 \bmod 6$ and $x \equiv 4 \bmod 18$

12. 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

13. Suppose $n = 187 = 11 \times 17$. According to Euler's Theorem:

    (a) $2^{100} \bmod n = 1$
    (b) $2^{160} \bmod n = 1$
    (c) $2^{186} \bmod n = 1$
    (d) $2^{188} \bmod n = 1$

14. Let g be a generator for the integers modulo p. The discrete logarithm problem is:

    (a) given y, find x with $y = x^g \bmod p$;
    (b) given x, find y with $y = x^g \bmod p$.
    (c) given y, find x with $y = g^x \bmod p$;
    (d) given x, find y with $y = g^x \bmod p$.

15. When public key cryptography is used for encryption:

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

16. The RSA encryption scheme often makes use of an algorithm known as OAEP. OAEP is:

    (a) a pre-processing method for messages providing randomness and redundancy
    (b) a symmetric-key encryption algorithm for use in hybrid encryption
    (c) a method to generate large prime numbers efficienctly
    (d) a method to speed up decryption given knowledge of the factors of the modulus

17. For the RSA encryption scheme a large modulus n is chosen, typically around 2048 bits in practice. To improve efficiency, this is often used together with value of:

    (a) $e = 2^{16}$
    (b) $d = 2^{16}$
    (c) $e = 2^{16} + 1$
    (d) $d = 2^{16} + 1$

18. In the basic Diffie-Hellman key exchange protocol, Alice sends $g^a \bmod p$ to Bob, while Bob sends $g^b \bmod p$ to Alice. They compute a shared secret of the form $g^{ab} \bmod p$. A limitation of the basic protocol is that:

    (a) neither Alice nor Bob knows who the key is shared with
    (b) an attacker can easily compute the shared secret from the exchanged messages
    (c) Bob can choose b to make the shared secret have a particular given value
    (d) the values g and p can only be used once

19. Cryptosystems based on the discrete logarithm problem, such as Diffie-Hellman key exchange, can be implemented in the integers modulo a prime p or in an elliptic curve group. Which of the following statements is true?

    (a) There is no known efficient algorithm to find elliptic curve discrete logarithms for quantum computers

    (b) Elliptic curve public keys can have multiple valid private keys

    (c) The square-and-multiply algorithm cannot be used in elliptic curve groups

    (d) Elliptic curve keys can typically be smaller for the same security level

20. The SHA-2 family of hash algorithms includes members which have hash output sizes of:

    (a) 16 bits, 24 bits, 48 bits and 56 bits

    (b) 100 bits, 200 bits, 250 bits and 300 bits

    (c) 64 bits, 128 bits, 224 bits and 256 bits

    (d) 224 bits, 256 bits, 384 bits and 512 bits

21. HMAC is an algorithm often used in TLS and based on a hash function H. Which of these statements with regard to HMAC is true?

    (a) The same secret key must be used to generate and to verify the HMAC tag

    (b) The size of the tag output by HMAC varies with the size of the input message

    (c) The message input to HMAC must be of a fixed length

    (d) The hash function H must have a 256-bit output size

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

    (a) one message has two different signatures

    (b) one signature is valid for two different messages

    (c) one message has two different hash values

    (d) two different hash values produce the same signature

23. An X.509 digital certificate is issued by a certification authority on behalf of a subject. In order to verify a certificate it is necessary to possess:

    (a) the private key of the subject

    (b) the public key of the subject

    (c) the public key of the certification authority

    (d) the private key of the certification authority

24. One type of key establishment protocol uses *key transport*: the session key is sent from a server to two parties to use to protect future communication. For this type of protocol:

    (a) a replay attack is always possible

    (b) forward secrecy is not possible

    (c) mutual authentication cannot be achieved

    (d) an active adversary can masquerade as any party

25. Kerberos is an authentication service which provides a *single sign-on* solution. This means that:

    (a) a user need only authenticate once in order to access many services during a defined period

    (b) a user needs to authenticate every time access to a server is required

    (c) only a single user is allowed to access a service at any one time

    (d) a single user is able to access services on behalf of other users

26. 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 messages

27. One TLS ciphersuite is denoted as TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. When this ciphersuite is chosen, ECDSA is used:

    (a) to sign the user data

    (b) to sign one or both Diffie–Hellman ephemeral values

    (c) to sign the server certificate

    (d) to sign the client certificate

28. TLS is often used to protect communication between a web browser and a server. A so-called "man-in-the-middle" attack is possible on TLS if the adversary is able to:

    (a) obtain the public key of the server's certification authority

    (b) eavesdrop on the key exchange messages

    (c) install new root certificates in the browser

    (d) obtain previously used session keys

29. PGP is a scheme for email security. One reason for the limited usage of PGP is:

    (a) PGP is not supported by most email servers

    (b) PGP does not allow signing of messages, only encryption of messages

    (c) PGP software is only legally available to US citizens

    (d) PGP users have difficulty in managing their public/private key pairs

30. One common way to apply the IPSec protocol uses a *host-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 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 simple random substitution cipher;
   - the random transposition cipher;

   Suppose that the alphabet used in each case has 27 characters and that the transposition cipher uses a block 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 each of these two ciphers can be attacked using a chosen plaintext attack. How much chosen plaintext would be necessary, in each case, to obtain all of the secret key using such an attack?

2. Cipher block chaining (CBC) mode for a block cipher, such as AES, is often used to form a message authentication code (MAC). Consider a different MAC algorithm using the CBC *decryption* equation: the MAC tag for a sequence of blocks $P_1, P_2, \ldots, P_n$ is the last block, T_n, using the following equation, where $P_0 = 00 \ldots 0$, the block of all zeros.

   $$T_t = D(P_t, K) \oplus P_{t-1}.$$

   (a) Explain how a receiver of the message $P_1, P_2, \ldots, P_n$, who has the shared key K, can check whether the accompanying tag T_n is correct.

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

3. 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 $p = 13$, the value 2 is a generator but the value 3 is not a generator.

   (b) Consider Diffie–Hellman key exchange in $\mathbb{Z}_p^*$ when $p = 13$ and $g = 2$. If principal A chooses random secret input value $a = 3$ and receives message $y = 8$ from B, what is the shared secret which they both obtain?

4. When using the RSA algorithm to form a digital signature, the output is a value $s = h(m)^d \bmod n$ for a suitable hash function h. The message m and s are sent to the verifier.

   (a) Given a valid public exponent e and the modulus n, how does the verifier check the signature?

   (b) Suppose now that the hash function is not used, so the signature for a message is simply $s = m^d \bmod n$. Explain how an attacker can construct a valid signature and message, without seeing any other signature.

5. Consider the following protocol with the goal of key establishment. Here N_A is a nonce chosen by A, T_B is a timestamp from the clock at S, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

   1. $A \to S : ID_A, ID_B, N_A$
   2. $S \to A : \{K_{AB}, ID_B, N_A\}_{K_{AS}}, \{K_{AB}, ID_A, T_B\}_{K_{BS}}$
   3. $A \to B : \{K_{AB}, ID_A, T_B\}_{K_{BS}}$

   (a) What is the purpose of including the identity ID_B in the first part of message 2? What attack could happen if it was not included?

   (b) Suppose that an attacker can control the clock at B and set it to any chosen value. Explain how this allows such an attacker can launch a replay attack on the protocol.

6. Two different protocols often used to protect email in transit are PGP and STARTTLS.

   (a) Consider the two following situations.

      i. You want to keep your email contents confidential from your email server.

      ii. You want to hide the *identity* of the person you are sending email to.

      Which of the two protocols can help you in each case? Explain your answers.

   (b) Both of PGP and STARTTLS can use public key cryptography with certified public keys. How do they differ with regard to the way public key certificates are validated?

TTM4135 Examination 2017-08-08
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) □

TTM4135 Examination 2017-08-08
Answer page for Exercise 1 Multiple Choice Questions

Detach this page and hand it in together with your written answers

Candidate number: □□□□□

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) □

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) □

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:
   (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) □

TTM4135 Spring exam 2020: Outline answers

1 Multiple choice questions

1 point for correct answer, 0.5 point penalty for incorrect answer. Explanation can say why one answer is correct, **or** why two answers are wrong for 1 point. Possible to get 0.5 point for explanation of why one answer is wrong.

1. Suppose that n is any odd number. Then $2^{-1} \bmod n$ is:

   (a) $n-2$

   (b) $(n+1)/2$ ✓

   (c) $(n-1)/2$

   Explanation: $2 \cdot (n+1)/2 \bmod n = n+1 \bmod n = 1$.

2. Suppose a plaintext comes from a natural language, similar to English, where the most frequent character appears with probability 1/10. For which of the following ciphers is the frequency of all ciphertext characters likely to be less than 1 in 10?

   (a) The random simple substitution cipher

   (b) A transposition cipher on blocks of size 12

   (c) The Vigenére cipher with a key of length 8 ✓

   Explanation: The Vigenére cipher smooths the frequency of the plaintext characters so we expect that the most frequent plaintext character will be split into ciphertext characters of lower frequencies.

3. Which of the following ciphers has the largest number of possible keys?

   (a) The triple-DES cipher with two independent keys

   (b) The random simple substitution cipher with alphabet consisting of all 8-bit bytes ✓

   (c) The AES block cipher with the shortest allowed key length

   Explanation: The alphabet for the simple substitution has 256 characters so there are 256! keys. A very crude estimate is that $256! >> 128^{128} = 2^{896}$ which is much more than the other two ciphers (or any modern standard cipher).

4. A block cipher is a function $E(m,k)$ which takes a plaintext block m and a key k to a ciphertext block c. In any useful block cipher:

   (a) for a fixed key k, the function $E(\cdot,k)$ is a permutation of the set of plaintext blocks ✓

   (b) for a fixed plaintext block m, the function $E(m,\cdot)$ is a permutation of the set of keys

   (c) for a fixed ciphertext block c, there is a unique pair (m,k) such that $E(m,k)=c$

Explanation: For a fixed k, there must be exactly one ciphertext block which is the encryption of any plaintext block, otherwise it would not be possible to decrypt.

5. Suppose the string `ABCDE` is a portion of a ciphertext which has been encrypted with the one time pad. The corresponding plaintext string P is another 5-character string. Which of the following is the most accurate statement?

   (a) Every possible plaintext string of length 5 is equally likely to be the correct P

   (b) The attacker gains nothing useful about the correct P from seeing `ABCDE` ✓

   (c) The correct P is the same plaintext corresponding to any previous portion of ciphertext equal to `ABCDE`

   Explanation: Although in general the plaintexts are not equally likely, the ciphertext from the one time pad does not help an attacker in guessing what was the correct plaintext.

6. The discrete logarithm problem in $\mathbb{Z}_p^*$ is the basis for many public key cryptosystems. On conventional computers (not quantum computers) there is:

   (a) no known polynomial time algorithm ✓

   (b) no known subexponential time algorithm

   (c) no known exponential time algorithm

   Explanation: The number field sieve is a sub-exponential time algorithm for the DLP in $\mathbb{Z}_p^*$.

7. The security of RSA encryption is related to the problem of integer factorisation in the following way:

   (a) if RSA cannot be broken then factorisation is hard ✓

   (b) if RSA can be broken then factorisation is easy

   (c) If RSA is secure then factorisation may be easy or hard

   Explanation: If factoring is easy then an attacker can find the RSA public key from the private key, so that RSA is definitely broken. This is the same as saying that if RSA cannot be broken than factorisation must be hard.

8. 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 ✓

Explanation: The owner of the private decryption key also can have access to p and q, allowing application of the CRT

9. ElGamal encryption works in $\mathbb{Z}_p^*$. The ciphertext of a message m is a pair (g^k, my^k). To avoid a known plaintext attack it is essential to:

   (a) choose a new k for each encryption ✓

   (b) choose a new y for each encryption

   (c) choose a new g for each encryption

   Explanation: Since y is the public key of the recipient, a new k must be chosen so that y^k is different for each message. If not then y^k can be extracted from one known plaintext/ciphertext pair and used to decrypt other messages.

10. Let h be the identity function, $h(x) = x$ defined on bit strings of length 128-bits. This function does not meet the property of being:

    (a) oneway ✓

    (b) collision-resistant

    (c) second pre-image resistant

    Explanation: Given an output value y we know that the input to h was also y, thus h is not one-way.

11. HMAC is a takes as input a key K and message M and outputs a tag T. Suppose that HMAC uses the hash function is SHA-256. If $HMAC(K, M_i)$ is computed for many different messages M_i (and a fixed K) then two identical tags will probably first appear after:

    (a) 2^{16} tag values are computed

    (b) 2^{128} tag values are computed ✓

    (c) 2^{255} tag values are computed

    Explanation: By the birthday paradox, collisions are likely to appear after around the square root of the number of possible tags have been computed, so around $2^{256/2}$.

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

    (a) a signature must be randomised but a MAC tag need not be

    (b) a MAC tag can be recomputed by the verifier but a signature cannot be ✓

    (c) a MAC provides data integrity but a signature does not

Explanation: The recipient of a MAC shares the key with the sender and can recompute to verify the tag; for a signature only the private key owner can compute signatures.

13. The Kerberos protocol makes use of a ticket containing four values $(K_{AB}, ID_A, ID_S, N_A)$ which is shared between a client A and server S. A suitable algorithm to use to protect these values would be:

    (a) AES in GCM mode ✓

    (b) AES in CBC mode

    (c) HMAC

    Explanation: The ticket needs to be confidential, to hide K_{AB}, and preserve integrity of the identities and nonce. Therefore AES in GCM mode is the only option.

14. 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

    Explanation: Only Diffie-Hellman handshakes are allowed in TLS 1.3 since the RSA method in TLS 1.2 was removed.

15. Many email servers add a DomainKeys Identified Mail (DKIM) digital signature to outgoing mail. This signature:

    (a) can be verified by any recipient of the email ✓

    (b) is verified and then removed by the receiving domain mail server

    (c) can only be verified by the receiving domain

    Explanation: The signature is openly available in the mail headers and can be verified by anyone using the public key which can be obtained from the DNS record.

2 Written answer questions

1. Consider a variant of the Hill cipher which has the encryption equation

$$C = KP + L \bmod n$$

where the key has two parts, a 2 × 2 matrix K and 2 × 1 column vector L. The column vectors C and P represent the ciphertext and plaintext respectively. Here n is the size of the alphabet in use. In this question all matrices are 2 × 2. If $L = 0$ then this variant is the same as the basic Hill cipher.

   (a) What is the decryption equation for this variant cipher?
   $P = K^{-1}(C - L) \bmod n$ (1 mark)
   Note that matrix multiplication is not commutative, so it matters in which order the computation is done.

   (b) What is the possible number of keys in this variant? Write an expression in terms of n and the number of keys of the basic Hill cipher.
   $n^2 \times N_{BH}$ where N_{BH} is the number of keys in the basic Hill. Not all matrices are valid for the basic Hill, so it is inaccurate to say that $N_{BH} = n^4$. (1 mark)

   (c) Explain how an attacker can use a chosen plaintext attack to obtain the key with three chosen plaintext pairs.
   Suppose that (P_1, P_2, P_3) are three plaintext column vectors with corresponding ciphertext vectors (C_1, C_2, C_3). Then

$$C_1 = K \cdot P_1 + L \tag{1}$$
$$C_2 = K \cdot P_2 + L \tag{2}$$
$$C_3 = K \cdot P_3 + L \tag{3}$$

   By setting $P_1 = 0$ (column vector) we can first find L since then $C_1 = L$. Then we can subtract L to get a square matrix equation: $((C_2 - L)(C_3 - L)) = K \cdot (P_2P_3)$ which can be solved as the basic Hill for K by inverting (P_2P_3). Note that in a chosen plaintext attack P_2 and P_3 can be chosen to ensure that (P_2P_3) is invertible. (3 marks)

2. A non-standard mode of operation for block ciphers has the following general equation for computing each output block: $C_t = E(P_t \oplus P_{t-1} \oplus C_{t-1}, K)$ where $C_0 = IV$ which is sent with the ciphertext and $P_0 = 0$ (the block of all 0 bits).

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

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

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

   (1 mark)

   Alternate answer

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

(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.

One bit change in C_t will give a random output for $D(C_t, K)$. So P_t will be random. But this randomness will also then propagate to P_{t+1} since P_t gets added in. Thus all subsequent plaintext blocks get changed randomly (but not independently). (2 marks)

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

To encrypt in parallel you need to have the previous C_{t-1} block so parallel encryption is not possible.

Parallel decryption is possible by first finding all the $D(C_t, K)$ values and then adding the previous P_{t-1} and C_{t-1} blocks. *(However, the statement that parallel decryption is not possible was also accepted.)* (2 marks)

Alternate answer:

To encrypt in parallel you need to have the previous C_{t-1} block so parallel encryption is not possible.

To decrypt in parallel you need to have the previous P_{t-1} block so parallel decryption is not possible.

3. Two efficient tests for primality of an integer n are the Fermat test and the Miller–Rabin test. Both tests use a base value a chosen randomly in the range $1 < a < n - 1$ and are usually run for multiple bases. Suppose that the tests are being used to test $n = 45$.

Alternate question: Numbers are $n = 85$ and $a = 4$

(a) Show that $19^2 \bmod 45 = 1$.

$19 \times 19 \bmod 45 = 361 \bmod 45 = 8 \times 45 + 1 \bmod 45 = 1$. (1 mark)

Alternate answer: $16 \times 16 \bmod 85 = 256 \bmod 85 = 1$.

(b) Show that the Fermat test will return that $n = 45$ is a probable prime if the value $a = 8$ is chosen.

$8^2 \bmod 45 = 19$. Thus from part (a), $8^4 \bmod 45 = 19^2 \bmod 45 = 1$

$8^{44} \bmod 45 = (8^4)^{11} \bmod 45 = 1$ (2 marks)

Alternate answer:

$4^2 \bmod 85 = 19$. Thus from part (a), $4^4 \bmod 85 = 16^2 \bmod 85 = 1$

$4^{84} \bmod 85 = (4^4)^{21} \bmod 85 = 1$

(c) Show that the Miller-Rabin test will return that $n = 45$ is composite if the value $a = 4$ is chosen.

$44 = 11 \times 4$. First compute

$8^{11} \bmod 45 = 8^8 \times 8^3 = 1 \times 19 \times 8 \bmod 45 = 152 \bmod 45 = 17$

$17^2 \bmod 45 = 19$

$19^2 \bmod 45 = 1$ (from part (a))

Since -1 never occurs in the sequence the Miller–Rabin test returns composite. (2 marks)

Alternate answer:

$84 = 21 \times 4$. First compute

$4^{21} \bmod 85 = 4^{20} \times 4 = 1 \times 4 \bmod 85 = 4$

$4^2 \bmod 85 = 16$

$16^2 \bmod 85 = 1$ (from part (a))

Since -1 never occurs in the sequence the Miller–Rabin test returns composite.

4. Consider the Diffie–Hellman protocol in the group $\mathbb{Z}_p^*$. In order to add authentication to the basic Diffie–Hellman protocol it is common to use digital signatures. An alternative is to use a long-term key directly in the protocol. Suppose that A has long-term secret key x with public key g^x and B has long-term secret key y with public key g^y. The protocol is then as follows.

   - A chooses random a and sends the value $A = g^a$ to B.
   - B chooses random b and sends the value $B = g^b$ to A.
   - A computes the session key $K_{AB} = B^x(g^y)^a$, using the received message Y and the long-term key of B.
   - B computes the session key $K_{BA} = A^y(g^x)^b$, using the received message X and the long-term key of A.

   (a) Show that A and B compute the same key: $K_{AB} = K_{BA}$.

$$\begin{aligned} K_{AB} &= B^x(g^y)^a \\ &= g^{bx}g^{ay} \\ &= g^{bx+ay} \end{aligned}$$

   By symmetry this is also equal to K_{BA}. (2 marks)

   (b) Show that this protocol does not achieve the forward secrecy property.

   We suppose that x and y are compromised after the session under attack is completed. Then the attacker has recorded A and B can compute:

$$\begin{aligned} K_{AB} &= A^x B^y \\ &= g^{ax+by} \end{aligned}$$

   (3 marks)

5. Two signature schemes commonly used today are RSA signatures and DSA signatures. Suppose that the RSA modulus n has length 2048 bits and the DSA modulus p has length 2048 bits with length of parameter q equal to 224 bits. You may assume that the DSA parameters p and q are fixed for all parties.

   Alternate question: Parameters are $|n| = 3072$, $|p| = 3072$, $|q| = 256$.

   (a) RSA signatures often use a public exponent $e = 2^{16} + 1$. Approximately how much faster on average is signature verification with this value of e compared to when e is randomly chosen e?

   With short exponent need only 17 multiplications. With random exponent around 3072. So ratio is around 192:1 (or 180 is more precise). (2 marks)

   Alternate answer: With short exponent need only 17 multiplications. With random exponent around 4608. So ratio is around 288:1 (or 271 is more precise).

   (b) What is the approximate ratio of the signature length, RSA against DSA?

   DSA has two components each size q, so 448 bits while RSA uses 2048 bits. So ratio is about 1:4.5. (1 mark)

   Alternate answer: DSA has two components each size q, so 512 bits while RSA uses 3072 bits. So ratio is about 1:6.

(c) What is the approximate ratio of the signing key length, RSA against DSA?

RSA key has size 2048 for private exponent. DSA has short exponent of 224 bits. So 9:1 approximately. *Also acceptable to include RSA modulus, when ratio becomes 18:1.* (1 mark)

Alternate answer: RSA key has size 3072 for private exponent. DSA has short exponent of 256 bits. So 12:1 approximately. *Also acceptable to include RSA modulus, when ratio becomes 24:1.*

(d) What is the approximate ratio of the verification key length, RSA against DSA?

RSA key has size 2048 for modulus, but could have fixed exponent. DSA has public key of 2048 bits. So 1:1 approximately. (1 mark)

Alternate answer: RSA key has size 3072 for modulus, but could have fixed exponent. DSA has public key of 3072 bits. So 1:1 approximately.

6. Protection of metadata, typically included in header information in network protocols, is important in preserving privacy.

(a) Compare what cryptographic protection is available for IP metadata in (i) IPSec in tunnel mode and (ii) TLS between a client and server.

In tunnel model IPSec encapsulates IP header information so that it is hidden from eavesdroppers. In contrast, TLS in normal usage does not touch IP headers since it works at the top of the transport layer (2 marks)

(b) Compare what cryptographic protection is available for email metadata in (i) PGP and (ii) STARTTLS.

PGP protects mail contents end-to-end without changing the headers which are necessary to deliver the mail. In contrast, STARTTLS works between mail servers and encapsulates the mail headers, but this protection relies on trust in the mail servers. (2 marks)

(c) Is there a conflict between protection of metadata and end-to-end security? Discuss such a conflict in the context of the above two examples.

IPSec in tunnel model and STARTTLS are not end-to-end and both encapsulate their payload to hide the metadata. However, end-to-end communication needs to use the header information, as with PGP and TLS. A solution is to use both. (1 mark)

TTM4135 exam May 2021: Outline answers

1 Multiple choice questions

1 point for correct answer, 0.5 point penalty for incorrect answer. Explanation can say why one answer is correct, **or** why two answers are wrong for 1 point. Possible to get 0.5 point for explanation of why one answer is wrong.

1. Suppose that $x^{-1} \bmod 17 = 5$. Then

   (a) $x \bmod 17 = 7$ ✓

   (b) $x \bmod 17 = 6$

   (c) $x \bmod 17 = 5$

   Explanation: $5 \times 7 \bmod 17 = 35 \bmod 17 = 1$

2. Suppose that the 26-letter alphabet, $A \dots Z$ is used for the plaintext in the 2×2 Hill cipher. Suppose that the letter E is the most common letter in the plaintext, occuring with frequency equal to 10%. Then in the ciphertext we can expect that:

   (a) the most common letter occurs with frequency equal to 10%

   (b) the most common letter occurs with frequency below 10% ✓

   (c) the most common letter occurs with frequency above 10%

   Explanation: Since the Hill cipher is simple substitution in pairs, each occurrence of the common characters can be encrypted in many ways, thereby smoothing the frequencies.

3. 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 much better ways to attack RSA than brute force key search ✓

   Explanation: Factorisation has sub-exponential time algorithms, so that factorising the modulus and then computing the private key directly from the public key, is much easier than brute for search for the private key.

4. Suppose that in a binary synchronous stream cipher a section of the ciphertext is 01000. An attacker knows that the plaintext used to obtain this ciphertext is 00101. The corresponding section of the decryption keystream is:

   (a) 01101 ✓

   (b) 00101

   (c) 01000

Explanation: Since $C = P \oplus K$ we can also calculate $K = P \oplus C = 00101 \oplus 01000 = 01101$.

5. Consider the version of the triple DES (3-DES) block cipher with three independent keys. Compared with the AES block cipher, this version of 3-DES:

   (a) has fewer possible keys than all versions of AES

   (b) has a shorter block length than all versions of AES ✓

   (c) is faster to run in software than all versions of AES

   Explanation: 3-DES has a 168-bit key length, so not shorter than AES 128, but has a 64-bit block length, so shorter than AES.

6. Suppose that you have a message of 100 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

   Explanation: ECB uses one 128-bit block; counter mode uses 100 bits + 64 for nonce; CBC uses 128 for ciphertext block and 128 bits for IV.

7. The Euler function ϕ is often useful for public key cryptography. It is true that:

   (a) $\phi(n)$ is always divisible by 3

   (b) if n is divisible by 3 then $\phi(n)$ is always divisible by 3

   (c) if n is divisible by 9 then $\phi(n)$ is always divisible by 3 ✓

   Explanation: $\phi(3) = 2$ rules out the first two options. If n is divisible by 3^2 then $2 * 3$ is a factor of $\phi(n)$.

8. Suppose you want to prevent an attacker from finding a collision in a hash function. The attacker has enough computing power to calculate 2^{40} hash values. You need to ensure that the attacker has only small chance of success but prefer the smallest acceptable output size. You have three possible output sizes to choose from. Which should you choose?

   (a) 40 bits

   (b) 64 bits

   (c) 128 bits ✓

Explanation: Due to the birthday paradox, with 2^{40} trials there is a good chance of a collision being found with an output of length even 80 bits. Therefore more than 80 bits is necessary

9. A message authentication code, MAC, takes as input a key K and message M and outputs a tag T. In order to be secure, it is essential that:

   (a) an attacker who knows a valid M and T cannot find K ✓

   (b) an attacker who knows a valid K and T cannot find M

   (c) an attacker who knows a valid K and M cannot find T

   Explanation: Knowing K allows forgeries. Therefore no secure MAC can leak K from knowledge of T and M which will be known to an attacker.

10. The RSA signature scheme uses a modulus n and a public exponent e. If the modulus is chosen to be $n = 13 \times 23 = 299$ (**corrected**) then the smallest valid choice for e would be

    (a) $e = 3$

    (b) $e = 5$ ✓

    (c) $e = 7$

    Explanation: $\phi(243) = 2 \times 12 \times 11$, so is divisible by 2, 3 and 4. The value of e must be prime to $\phi(n)$ for the private key to exist.

11. For efficiency reasons it is often useful to keep fixed parameter values for many users of a cryptographic scheme. Which of the following is *not* a practical choice for digital signatures?

    (a) RSA signatures with a fixed modulus n ✓

    (b) DSA signatures with fixed generator g and fixed modulus p

    (c) ECDSA signatures with a fixed elliptic curve group

    Explanation: Knowledge of one RSA signing/verification key is enough to factorise n. It is normal to re-use the parameters for DSA and ECDSA.

12. When assessing the security of a key establishment protocol, such as the Needham–Schroeder protocol, we assume that an attacker is able to:

    (a) re-send messages sent in any previous runs of the protocol ✓

    (b) force parties to re-use nonces used in previous runs of the protocol

    (c) obtain long-term keys used in any previous runs of the protocol

Explanation: We assume that the network is controlled by the attacker who can then send any known values to the users. Nonces are chosen by users and cannot be controlled by the attacker. Long-term keys usually are static and a protocol cannot be secure in the future once long-term keys are known.

13. In the TLS 1.2 handshake protocol, a ciphersuite is negotiated between the client and the server. Which of the following does *not* depend on the chosen ciphersuite:

    (a) the algorithm used to authenticate the record layer data

    (b) the algorithm used to sign the server key exchange message

    (c) the algorithm used to sign the server certificate ✓

    Explanation: Only the algorithms used actively in the handshake and record protocol are negotiated. The certificate is signed beforehand.

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

    (a) clients can send a Diffie–Hellman ephemeral value before the ciphersuite is agreed ✓

    (b) checking of server certificates is no longer required

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

    Explanation: TLS 1.3 allows optimistic sending of the client key exchange message in the first flow, before the ciphersuite is decided.

15. PGP is a security protocol to protect emails in transit. PGP has seen very limited usage in practice. One of the reasons for this is:

    (a) usability is a challenge for many potential users ✓

    (b) encryption is provided but it is not possible to authenticate mail senders

    (c) PGP-encrypted mail cannot be sent on the normal email system

    Explanation: PGP is transparent to mail servers and has optional signatures. It is notoriously hard for the average user to configure.

2 Written answer questions

1. Suppose that you share a new (unused) random key of 128-bits with a recipient. You are considering whether to use the key either as a one-time pad or with the AES block cipher in ECB mode.

   (a) Suppose first that you have a single message to encrypt, written in English as 16 × 8-bit bytes to make 128 bits in total. For this part assume that the key is used only once for this message. Compare the security of each of the two choices. Is one better than the other and why?

   (b) Now suppose that you have a second message to encrypt, also written in English as 16 × 8-bit bytes. You decide to use the same encryption method with the same key as you used for the first 128-bit message. Again, compare the security of the two choices.

   One time pad gives perfect secrecy. For a single block, ECB mode is also secure except against brute force key search. When used twice, the OTP is no longer secure, and in fact by XORing the two blocks the XOR of the two messages is obtained. Using ECB is also leaking some information, in particular if they are the same or different.

2. The Feistel construction for a block cipher uses the round equations:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   for some function f. Suppose that f is chosen to be the function:

$$f(R, K) = R \oplus K$$

   for any half-block, R, and any round key, K.

   (a) Show that with this choice of f it follows that for all $i \geq 2$, both of the following equations hold.

$$\begin{aligned} R_i &= L_{i-2} \oplus K_{i-1} \oplus K_i \\ L_i &= L_{i-2} \oplus R_{i-2} \oplus K_{i-1} \end{aligned}$$

   We have from the Feistel equations:

$$\begin{aligned} R_i &= L_{i-1} \oplus R_{i-1} \oplus K_i \\ &= R_{i-2} \oplus L_{i-2} \oplus R_{i-2} \oplus K_{i-1} \oplus K_i \\ &= L_{i-2} \oplus K_{i-1} \oplus K_i \end{aligned}$$

$$\begin{aligned} L_i &= R_{i-1} \\ &= L_{i-2} \oplus R_{i-2} \oplus K_{i-1} \end{aligned}$$

(b) Use the above observation to show how to break a 2-round Feistel cipher with this f function given one known plaintext/ciphertext pair.

Given $C = (L_2, R_2)$ we know that $L_2 = L_0 \oplus R_0 \oplus K_1$ and $R_2 = L_0 \oplus K_1 \oplus K_2$. Since $P = (L_0, R_0)$ is also known, this allows the round keys K_1 and K_2 also to be found, so that any other ciphertexts can be decrypted.

(c) Explain, just giving the idea, how part (ii) can be generalised to break a Feistel cipher with any even number of rounds if this f function is used.

Each (L_i, R_i) pair can be replaced with (L_{i-2}, R_{i-2}) plus a fixed round key combination. This can be done recursively to get back to $P = (L_0, R_0)$.

3. One non-trivial square root of 1 modulo 209 is 153.

Alternate question:

One non-trivial square root of 1 modulo 221 is 118.

(a) What are all four of the square roots of 1 modulo 209?

The trivial square roots are 1 and -1. Others are 153 and $-153 \bmod 209 = 56$.

Alternate question:

What are all four of the square roots of 1 modulo 221?

The trivial square roots are 1 and -1. Others are 118 and $-118 \bmod 221 = 103$.

(b) Choose one of your non-trivial square roots, x and show, using the Euclidean algorithm, that $\gcd(x + 1, 209) > 1$.

Find $\gcd(57, 209)$.

$$\begin{aligned} 209 &= 3 \times 57 + 38 \\ 57 &= 38 + 19 \\ 38 &= 2 \times 19 \end{aligned}$$

So $\gcd(57, 209) = 19$ which is a divisor of 209

Alternate question:

Choose one of your non-trivial square roots, x and show, using the Euclidean algorirhm, that $\gcd(x + 1, 221) > 1$.

Find $\gcd(104, 221)$.

$$\begin{aligned} 221 &= 2 \times 104 + 13 \\ 104 &= 8 \times 13 \end{aligned}$$

So $\gcd(104, 221) = 13$ which is a divisor of 221

(c) Explain how an efficient algorithm to find non-trivial square roots can be used to break the RSA cryptosystem.

Given the RSA modulus n, the above process can be used to factorise n given a non-trivial square root. This allows $\phi(n)$ to be computed and the private key to be found from the public key.

4. The normal RSA cryptosystem uses modulus $n = pq$, a decryption exponent, d, and public exponent, e. Suppose that a company wants to protect its private exponent so that no single entity can decrypt. The manager splits d into two parts, d_1, d_2 such that

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

In order to decrypt a ciphertext C, entity E_1 computes $M_1 = C^{d_1} \bmod n$, entity E_2 computes $M_2 = C^{d_2} \bmod n$ and these are combined to form $M = M_1 \times M_2 \bmod n$.

Alternate question:

The normal RSA cryptosystem uses modulus $n = pq$, a decryption exponent, d, and public exponent, e. Suppose that a company wants to protect its private exponent so that no single entity can decrypt. The manager splits d into two parts, d_1, d_2 such that

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

In order to decrypt a ciphertext C, entity E_1 computes $M_1 = C^{d_1} \bmod n$, entity E_2 computes $M = M_1^{d_2} \bmod n$.

(a) Show that a ciphertext encrypted with normal RSA, with public key e and n, is decrypted properly with this method. (You may assume that normal RSA works correctly.)

$M_1 \times M_2 \bmod n = C^{d_1} \times C^{d_2} \bmod n = C^{d_1+d_2} \bmod n = C^d \bmod n = M$, applying Euler.

$M_1^{d_2} \bmod n = (C^{d_1})^{d_2} \bmod n = C^{d_1 d_2} \bmod n = C^d \bmod n = M$, applying Euler.

(b) This system runs slower than normal RSA. To improve the efficiency the manager decides to give both E_1 and E_2 the values p and q so that they can use the CRT to decrypt.

i. Does this make the system as fast as normal RSA? Explain your answer.

ii. Why does this defeat the purpose of the system?

Use of the CRT speeds up decryption by a factor of around 4 times. The system is now almost as fast as plain RSA since the decryptions can be run in parallel. But either party can recover the whole of d and decrypt alone.

Alternate answer: The system is now almost half as fast since the decryptions cannot be run in parallel. But either party can recover the whole of d and decrypt alone.

5. Consider the following protocol with the goal of key establishment. This is a repaired version of the Needham–Schroeder protocol.

Here N_A is a nonce chosen by party A, N_B is a nonce chosen by B, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_{AS} and K_{BS} are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

1. $A \rightarrow B : ID_A, N_A$
2. $B \rightarrow S : ID_A, ID_B, N_A, N_B$
3. $S \rightarrow B : \{N_A, ID_A, ID_B, K_{AB}\}_{K_{AS}}, \{N_B, ID_A, ID_B, K_{AB}\}_{K_{BS}}$
4. $B \rightarrow A : \{N_A, ID_A, ID_B, K_{AB}\}_{K_{AS}}$

(a) On receipt of message 4, A should check that the received N_A is the same value as that chosen in message 1. Describe an attack on the protocol if A does not perform this check, including the messages which an attacker sends. What is the consequence of this attack?

Attacker can replay old messages and this would not be detected by A. The attacker can capture $\{N_A, ID_A, ID_B, K'_{AB}\}_{K_{AS}}$ from a previous protocol run, obtain the old session key K'_{AB}, and then it will be accepted by A.

(b) On receipt of message 3, B should also check that the received ID_A is the same identity received in message 1 and sent in message 2. Describe an attack if B does not perform this check.

Attacker can change the identity in message 2 so that B shares the key with, say, C instead of A.

Alternate question:

(b) Suppose that instead of using authenticated encryption, plain encryption by a synchronous stream cipher is used, such as AES in counter mode. How does this also allow an attack?

Attacker can change any known field. For example, ID_B can be changed to ID_C in message 4 by adding in $ID_B \oplus ID_C$. This will trick A to think the key is shared with C instead of B.

6. The Signal messaging protocol uses two kinds of *ratcheting* to update the keys used to protect messages: Diffie–Hellman ratcheting is used when the next message is sent in the opposite direction from the previous message; symmetric ratcheting with a hash function is used when the next message is sent in the same direction. Assume a powerful adversary who can capture and delay messages and has the ability to compromise devices later.

(a) How does the ratcheting in Signal improve the security of messages against this adversary, in comparison to the security of:

i. email messages encrypted with PGP;
There is no forward secrecy for PGP encryption, so the adversary will obtain all previous messages.

ii. messages sent as application data in a TLS 1.3 session.

The main difference is that a different key is used to protect each message. If a device is compromised, only the key to protect the current message will be revealed. Older messages cannot be found.

(b) If several messages are sent in the same direction in the Signal protocol, how does their security compare to the security of messages sent successively in opposite directions?

An adversary who delays messages and compromises the recipient can obtain all of the messages sent in the same direction. The adversary can only obtain the messages obtained after the compromise since the ratchet is one-way. There is also a (system imposed) limit on how many consecutive messages you can send before you are forced to do a DH-ratchet up and down.

TTM4135 exam August 2021: Outline answers

1 Multiple choice questions

1 point for correct answer, 0.5 point penalty for incorrect answer. Explanation can say why one answer is correct, **or** why two answers are wrong for 1 point. Possible to get 0.5 point for explanation of why one answer is wrong.

1. Suppose that $3x = kn + 1$ for positive integers x, k and n. Then it follows that:

   (a) $3^{-1} \bmod n = x \bmod n$ ✓

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

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

   Explanation: $3x \bmod n = kn + 1 \bmod n = 1$

2. Two historical ciphers are the simple substitution cipher and the Vigenère cipher. Suppose that the 26-letter alphabet, $A \dots Z$ is used for the plaintext and that the Vigenère cipher has a key of length 5. Which of the following is true?

   (a) The Vigenère ciphertext will most likely have a flatter (more uniform) frequency distribution than the simple substitution ciphertext ✓

   (b) The Vigenère cipher has more possible keys than the simple substitution cipher

   (c) The most frequent character in the Vigenère ciphertext will most likely be same as the most frequent character in the simple substitution ciphertext

   Explanation: The Vigenére cipher substitutes each plaintext character with different ciphertext characters resulting in a flatter distribution, in contrast to the simple substitution cipher which preserves the letter frequencies.

3. Suppose that in a binary synchronous stream cipher a section of the keystream is 01101. An attacker knows this keystream and intercepts the corresponding ciphertext 00101. The corresponding section of the plaintext is:

   (a) 01000 ✓

   (b) 00101

   (c) 01101

Explanation: Since $C = P \oplus K$ we can also calculate $P = K \oplus C = 01101 \oplus 00101 = 01000$.

4. The DES block cipher and the AES block cipher differ in the following way:

   (a) AES has only one round function but DES uses several different round functions

   (b) AES has only one S-box but DES uses several different S-boxes ✓

   (c) AES has only one round key but DES uses several different round keys

   Explanation: Both AES and DES are iterated ciphers with different round keys and a fixed round function. AES has only one large S-box.

5. Suppose that you have a message of 160 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

   Explanation: ECB uses two 128-bit blocks so 256 bits; counter mode uses 160 bits + 64 bits for nonce so 224 bits; CBC uses two 128 ciphertext blocks and 128 bits for IV so 384 bits.

6. Suppose you want to prevent an attacker from finding a collision in a hash function. The attacker has enough computing power to calculate 2^{80} hash values. You need to ensure that the attacker has only a small chance of success but you prefer the smallest acceptable output size. You have three possible output sizes to choose from. Which should you choose?

   (a) 128 bits

   (b) 256 bits ✓

   (c) 384 bits

   Explanation: Due to the birthday paradox, with 2^{80} trials there is a good chance of a collision being found with an output of length 160 bits. Therefore more than 160 bits is necessary.

7. A message authentication code, MAC, takes as input a key K and message M and outputs a tag T. Suppose an attacker observes a valid tag T for a known message M. In order to be secure, it is essential that:

   (a) the attacker cannot find a valid T for the same M and a different K

   (b) the attacker cannot find a valid M for the same T and a different K

(c) the attacker cannot find a valid T for the same K and a different M ✓

Explanation: Finding a new valid T with the same K is a forgery. For a different K the attacker can choose the key so this is not a forgery.

8. The Euler function ϕ is often useful for public key cryptography. Suppose that $n = 143 = 11 \times 13$. Then for any a, it is true that:

   (a) $a^{150} \equiv a^{30} \bmod n$ ✓

   (b) $a^{150} \equiv a^{8} \bmod n$

   (c) $a^{150} \equiv a^{15} \bmod n$

Explanation: $\phi(n) = 120$ so by Euler $a^x \bmod n = a^{x+120} \bmod n$.

9. A typical RSA private key in use today may have length 3072 bits, but a typical elliptic curve private key may have length around 256 bits. This longer key for RSA is necessary because:

   (a) security for RSA encryption needs to be stronger than for elliptic curve encryption (such as ElGamal encryption on elliptic curves)

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

   (c) there are faster algorithms known to solve the factorisation problem than there are to find elliptic curve discrete logarithms ✓

Explanation: Factorisation has sub-exponential time algorithms, but we only know exponential time algorithms for the EC discrete logarithm problem.

10. Consider the following encryption scheme, which is similar to, but different from, the ElGamal encryption scheme. A ciphertext for message m has two parts: $C_1 = m \cdot g^k \bmod p$ and $C_2 = y^k \bmod p$, where $y = g^x$ is the recipient public key. In order to recover the message, the recipient must compute $z = x^{-1} \bmod (p-1)$ and then:

   (a) $m = C_1 \cdot (C_2^z)^{-1} \bmod p$ ✓

   (b) $m = C_2 \cdot (C_1^z)^{-1} \bmod p$

   (c) $m = C_1^z \cdot (C_2)^{-1} \bmod p$

Explanation: $C_2^z \bmod p = y^{kz} \bmod p = g^{xkx^{-1} \bmod (p-1)} \bmod p = g^k \bmod p$. Therefore $C_1 \cdot (C_2^z)^{-1} \bmod p = m \cdot g^k \bmod p / g^k \bmod p = m$.

11. The RSA signature scheme often uses a public exponent $e = 2^{16} + 1$. Instead we could try to use a private exponent $d = 2^{16} + 1$ to increase the speed of signature generation. This would not be a good idea because:

    (a) it would not be possible to find the correct public exponent e

    (b) an attacker could easily forge signatures ✓

    (c) the Chinese Remainder Theorem could no longer be used to increase the speed of signature generation

    Explanation: If it is know that a fixed d is used, then with the modulus (part of the public key) forging signatures is trivial.

12. The Kerberos V5 security protocol provides authentication and key establishment using an online authentication server (AS) which shares a long-term key with each user. A limitation this protocol is:

    (a) forward secrecy is not provided ✓

    (b) an attack is possible involving replay of a previously used session key

    (c) users need to obtain certified public keys in order to use the protocol

    Explanation: If a user long-term key is compromised then tickets from the AS can be decrypted to obtain the key used. So forward secrecy is not provided. The attack on Needham–Schroeder is not valid on Kerberos due to the use of timestamps in tickets. Public keys are not used.

13. When TLS is used to protect web browser communications with HTTPS, a set of root certificates comes with the browser. The keys from these root certificates are used to:

    (a) verify server certificates sent in the TLS handshake protocol ✓

    (b) sign Diffie-Hellman ephemeral keys used in the TLS handshake protocol

    (c) encrypt the pre-master secret sent in the TLS handshake protocol

    Explanation: The root certificates are the root of security (authenticity) so that the signatures in server certificates can be verified. The server public key is used for signing Diffie-Hellman shares or, in the RSA case for TLS 1.2, encrypt the pre-master secret.

14. In typical usage of tunnel mode, the IPSec protocol provides:

    (a) protection of user metadata ✓

    (b) end-to-end security of user data

    (c) non-repudiation of user data

Explanation: IPSec in tunnel mode is typically used for gateway-to-gateway architectures. The original IP header is encapsulated in a new IP packet and hidden from eavesdroppers.

15. PGP is a security protocol to protect emails in transit. One limitation of PGP is:

    (a) a corrupted mail server is able to read the contents of PGP-encrypted mail

    (b) a corrupted mail server can reveal the metadata such as sender and recipient identities ✓

    (c) a corrupted mail server can forge valid PGP signatures on behalf of any message sender

Explanation: PGP provides end-to-end security but must leave headers intact to allow routing of the message.

2 Written answer questions

1. Consider the following version of the historical Vigenère cipher. The alphabet consists of 64 characters (for example, 52 lower and upper case letters, 10 digits, full stop and comma). Encryption of each plaintext character p_i consists of a shift defined by a key character k_i. The key K is specified by a sequence of 20 characters: $K = k_0 \dots k_{19}$ where k_i for $i = 0, \dots, 19$ gives the amount of shift in the ith alphabet, i.e.

$$c_i = p_i + k_{i \bmod 20} \bmod 64.$$

   (a) How many possible keys does this cipher have?

   (b) By comparing with the AES block cipher, explain how secure this cipher would be against brute force key search.

   (c) Explain how this cipher is easily broken with a known plaintext attack. Include an estimate of how much known plaintext would be needed.

   (a) There are 64 possible shifts for each key character, so in total there are 64^{20}.

   (b) The number of possible keys is 2^{120} which is equivalent to a 120-bit key, only 8 bits smaller than AES-128 keys. Therefore this cipher is reasonably secure against brute force key search attack .

   (c) With a known plaintext attack, an attacker can see the amount of shift for each key position. The whole key can be recovered from 20 consecutive characters of known/chosen plaintext.

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:

$$C_t = O_t \oplus P_t$$

   where $O_t = E(T_t \oplus C_{t-1}, K)$ 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).

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

   $P_t = C_t \oplus O_t$. (Note that no decryption is required.)

   (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.

   One bit change in C_t will change one bit in the decrypted P_t and change O_{t+1} to be a random block. Thus the next block P_{t+1} will be decrypted as a random block. However, assuming C_{t+1} is correct, O_{t+2} will be correct again and so all following blocks are not affected. Thus only one plaintext block has one bit changed and the following plaintext block is changed to random.

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

   To encrypt in parallel you need to have the previous C_{t-1} block so parallel encryption is not possible.

   To decrypt in parallel you already have the previous C_{t-1} block so parallel decryption is possible.

3. A message authentication code (MAC) takes an input message M and key K and computes a tag T. Consider a MAC defined using a block cipher decryption function D with a 128-bit shared key K:

$$\mathrm{MAC}(M, K) = T = D(M, K).$$

This MAC is only defined for messages of exactly 128 bits in length.

(a) Explain how this MAC should be verified by a recipient of a pair (M, T).

The recipient simply recomputes the tag and checks that its computation is the same as the received T. For this MAC the recipient can also encrypt the tag and check that this yields the received message.

(b) Explain why it should be difficult for an attacker to find a valid tag for a given message M, even after seeing many valid message/tag pairs (M_i, T_i) for a fixed K and messages M_i different from M.

To find a valid tag, the attacker needs to decrypt the "ciphertext" M with key K. This should not be possible for a good block cipher. Moreover, a good block cipher should be still be secure given many ciphertext plaintext pairs, which correspond to the (M_i, T_i) pairs.

(c) Suppose that the MAC is now re-defined to allow any message of 256-bits by dividing the 256-bit input M into two 128-bit sub-blocks M_1, M_2 and defining $T = D(M_1 \oplus M_2, K)$. Explain why it is now easy for an attacker to find a forgery given just one valid pair (M, T)

A message M is now two 128-bit blocks, M_1, M_2. But given any such message, the tag T will remain the same by replacing these with M_1', M_2' where $M_1 \oplus M_2 = M_1' \oplus M_2'$. Thus an attacker can choose any M_1' and compute $M_2' = M_1' \oplus M_1 \oplus M_2$ and then the tag T is valid for this new message.

4. The Miller–Rabin algorithm is often used for generation of prime numbers in public key cryptography. A related, but simpler, algorithm is known at the Fermat test. These two tests are compared in this question. Show your working for the computations, which should all be straightforward without use of a calculator.

(a) Show that $2^{10} \bmod 341 = 1$ and deduce that 32 is a non-trivial square root of 1 modulo 341. Use this result to find a factor of 341.

$2^{10} \bmod 341 = 1024 \bmod 341 = 3 \times 341 + 1 \bmod 341 = 1$. Therefore $2^{10} \bmod 341 = (32)^2 \bmod 341 = 1$ and since 32 is different from 1 and -1 it is a non-trivial square root. $\gcd(31, 341)$ must be a factor of 341. $341 = 11{*}31$. (Alternatively, $\gcd(33, 341)$ must be a factor of 341. $341 = 11{*}31$.)

(b) Show that the Fermat test will decide that 341 is a probable prime when the base is chosen as 2.

The Fermat test will compute: $2^{340} \bmod 341 = (2^{10})^{34} \bmod 341 = 1$ so the Fermat test is passed.

(c) Show that the Miller–Rabin test correctly identifies 2 as a composite number.

Since $340 = 85 \times 2^2$, the Miller–Rabin test will compute: $2^{85} \bmod 341 = (2^{10})^8 \times 2^5 \bmod 341 = 32$ and then $32^2 \bmod 341 = 1$. So the M-R test finds the non-trivial square root 32 and identifies 341 as composite.

5. Two digital signature algorithms often used in network security protocols are: RSA signatures and DSA signatures. Suppose that these signatures both use a modulus of size 3072 bits.

Alternate question: Suppose that these signatures both use a modulus of size 4096 bits.

(a) What are the total sizes of the public information needed to verify a signature from each of the two schemes? Show separately the sizes of all different components, including all of the public parameters that would be needed in order to complete the verification.

(b) Suppose that signatures from many different signers will be verified so that some parameters may be shared between different signers. For each of the two signature schemes, state which public parameters cannot be shared and explain why they cannot. What is the size of the public key components that must be different for each signer?

(a) RSA: modulus n: 3072 bits; verification exponent e: 17 bits or random 3072 bits. Total 3089 bits or 6144
DSA: modulus p: 3072 bits; generator g: 3072 bits; public key y: 3072 bits. Total 9216 bits.

(b) RSA modulus cannot be fixed, but public exponent can be fixed. 3072 bits for each user. DSA can fix p and g. 3072 bits for each user.

6. The following ciphersuite for TLS 1.2 is classified as *weak* (for example by SSL Labs):

TLS_RSA_WITH_AES_256_GCM_SHA384

Alternate question: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

This question concerns comparison with the following TLS 1.3 ciphersuite:

TLS_AES_128_GCM_SHA256

(a) Compare the security of these two ciphersuites, commenting on each of the algorithms used for handshake and for record layer security. Why is the TLS 1.2 ciphersuite weak while the TLS 1.3 ciphersuite is not?

In the handshake protocol TLS1.3 ciphersuites always use ECDHE which gives forward secrecy. Using RSA in the handshake does not provide forward secrecy which is why it is classified as weak. The record layer algorithms are actually stronger in the TLS 1.2 ciphersuite since they used longer key lengths.

Alternate answer: In the handshake protocol TLS1.3 ciphersuites always use ECDHE so in fact both ciphersuites specify the same handshake algorithms. which is why it is classified as weak. The record layer algorithms are the same in the TLS 1.2 and TLS 1.3 ciphersuites but the key derivation functions for the TLS 1.2 ciphersuite will use SHA which has been broken (collisions found) which is why it is classified as weak.

(b) How will the security of these two ciphersuites be affected if quantum computers become available to attackers in the future? Is there a difference between the security of sessions which happen *before* the attackers have the quantum computer and those which happen afterwards?

Quantum computers will allow breaking of both factorisation and ECDLP problems, so both ciphersuites will be broken. It does not matter much whether the session happens before or after quantum computers become available, except that attackers will need to record and store the TLS protocol messages for those session of interest. So storage is required for sessions before quantum computers exist.