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.

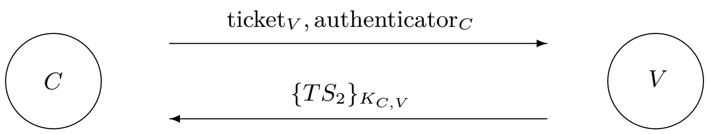
   (a) Explain how a recipient of a message M and a tag T should check the integrity of the received message.

   (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) ☐