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 $\gcd(a, n) = 1$.

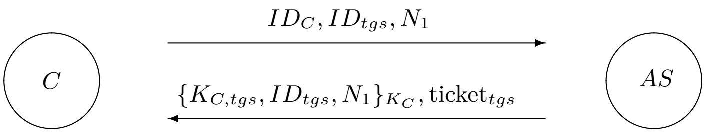
   (a) Illustrate the theorem using one example with respect to the prime $p = 23$.

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

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