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?

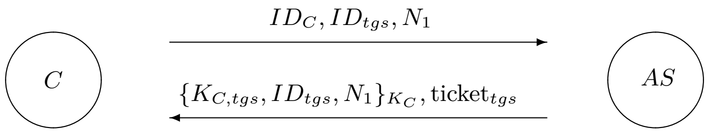
   (b) If n and b are 2400 bits in length, what is the expected number of squarings and multiplications needed to apply the square-and-multiply method?

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) ☐