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) ☐