Mid-term Exam
Information Security, 08 March 2018, 13:30-15:30
(13:30-16:00 for students with extra time)

You can score a maximum of 100 points and you have 120 minutes to solve all 10 questions.

Your answers must be in English.
You are NOT allowed to use books/slides/notes/*etc.* as well as a (smart) phone or any other devices.
Non-graphics calculator may be used.
Please use a separate sheet of paper to make drafts and pre-calculations.
Write your final answer clearly on the exam questionnaire.
Do not forget to put **your name and student number on each sheet**.

Good luck!

— This page intentionally left blank —

1. **(22 points)** Answer the following questions:

   (a) There are two types of assets that information and computer security aims to protect: software and hardware

   A. True
   B. False

   Answer:

   (b) The three basic elements of access control are

   A. Subject, objects and permissions
   B. Objects, access modes and rights
   C. Subjects, objects and access modes
   D. Subjects, access modes and permissions

   Answer:

   (c) Skimming is the use of a/an (i) ..... to (ii) ..... authentication data without being noticed

   A. device
   B. password
   C. mobile phone
   D. move
   E. delete
   F. copy

   Answer: (i)....., (ii) .....

   (d) Determine which of the following characteristic(s) apply to AES

   A. The block size is 128 bits
   B. It operates only with 16 rounds
   C. It employs bit shifting as an encryption primitive
   D. The key length can reach 112 bits with multiple keys

   Answer:

   (e) Determine which of the following statements about network protocols is **true** or **false**:

   A. They provide the details on how communication is accomplished
   B. They enable the independence between communications and the communication medium
   C. They are conventions for computers to interact

   Answer: A....., B....., C.....

   (f) Indicate which of the following statements is **true** or **false**? An intrusion detection system:

   A. looks for intrusions before the packets are inspected by the firewall
   B. if host-based, it is installed on a dedicated machine that protects the entire network
   C. operates before an attack has begun

   Answer: A....., B....., C.....

(g) An attacker exploits a/an (i) ..... in order to cause a/an (ii) .....
A/an (iii) ..... blocks a vulnerability by removing or reducing the effect of a/an (iv) .....

A. attacker
B. vulnerability
C. threat
D. countermeasure
E. defender
F. obstacle
G. bug

Answer: (i)....., (ii) ....., (iii) ....., (iv) .....

(h) How many attack attempts are necessary in the worst case to decrypt a message written in English encrypted with the Caesar cipher?
Answer: .....

(i) Determine whether the following statements refer to **block ciphers** or **stream ciphers**

A. The input symbols are transformed one at a time
B. The speed of transformation is high because symbols are encrypted as soon as they are read
C. Padding is typically required for most messages

Answer: A....., B....., C.....

(j) In an echo-chargen attack, the attacker sets up a/an (i) ..... on one machine that generates a/an (ii) ..... that targets another machine. This creates a/an (iii) ..... between two machines.

A. large packet
B. chargen process
C. echo packet
D. echo process
E. communication loop
F. smurf process
G. vulnerability
H. authentication problem

Answer: (i)....., (ii) ....., (iii) .....

2. **(6 points)** If you forget your password for a website and click `Forgot my password`, sometimes the company/service provider sends you a new password by email but sometimes it sends you your old password by email. Compare these two cases in terms of vulnerability of the website and its backend.

3. **(5 points)** IPsec can enforce confidentiality and/or authenticity via two modes of operation. State and briefly describe each of them, including how the recipient's address is protected.

4. **(3 points)** Does a VPN use link encryption and/or end-to-end encryption? Justify your answer.

5. **(6 points)** Consider circuit switching and packet switching. What are the benefits of each of them? Mention at least two for each.

6. **(4 points)** A circuit in a link is implemented with either frequency division multiplexing (FDM) or time-division multiplexing (TDM). What is the main difference between FDM and TDM? What are particular circuits assigned to?

7. **(9 points)** You receive an email message that claims to come from your bank. It asks you to click a link for some reasonable-sounding administrative purpose.

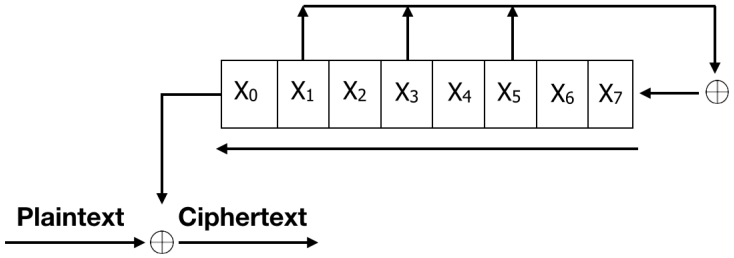
   (a) How can you verify that the message did come from your bank?

   (b) Now play the role of an attacker. How could you intercept the message described in part (a) and convert it to your purposes while still making both the bank and the customer think the message is authentic and trustworthy?

8. **(14 points)** State and briefly describe the different layers of the OSI reference model, and give an example of a protocol used at each layer.

9. **(12 points)** Consider the following simple Linear Feedback Shift Register (LFSR). The plaintext is bitwise XOR-ed with the output bits of the LFSR which **first computes** $X_1 \oplus X_3 \oplus X_5$ and **then shifts** such that X_0 falls out.

   Compute the next three states of the LFSR given the initial state `00111010`. You need to **clearly show** (i) each state, (ii) the output bit, and (iii) your XOR computation.



10. **(19 points)** Alice has chosen primes, $p = 17$ and $q = 23$, and encryption exponent, $e = 5$ as her RSA parameters.

    (a) Alice digitally signs message $m = 10$ and sends it to Bob. Show all the intermediate steps of your solution and **explicitly** mention what Alice sends to Bob.

    (b) Bob receives the signed message and proceeds to verify it. Show how Bob can verify that the message was indeed signed by Alice. Write down all the intermediate steps of your solution.

. . . . . **This is the end of the mid-term exam.** . . . . . .