Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 3103 CRYPTOGRAPHY II

DATE: 22nd July 2024 Time: 13:00-15:00 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE (30 MARKS)

a) Explain the main challenges associated with key distribution and key agreement in cryptographic systems. Provide examples of protocols used to address these challenges. (**6 Marks**)

b) Discuss the components of Public Key Infrastructure (PKI) and their roles in ensuring secure communications. (**6 Marks**)

c) Define and contrast Access Control Lists (ACLs) and Role-Based Access Control (RBAC) in the context of access control. Provide examples of scenarios where each would be appropriately applied. (**6 Marks**)

d) Describe the Needham-Schroeder Protocol and discuss a known vulnerability of this protocol. How was this vulnerability addressed in subsequent protocols? (**6 Marks**)

e) Explain how homomorphic encryption works and discuss its potential applications. Provide an example of a situation where homomorphic encryption would be particularly useful. (**6 Marks**)

QUESTION TWO (15 MARKS)

a) Discuss the concept of zero-knowledge protocols and provide an example of how such a protocol can be used in secure authentication. (**4 Marks**)

b) Explain the differences between S/MIME and PGP in email security. Which scenarios would benefit from the use of each technology? (**4 Marks**)

c) Describe the SSL/TLS protocol and its role in securing internet communications. Highlight the main phases of an SSL/TLS session. (**4 Marks**)

d) Analyze the role of salts and one-time passwords in enhancing password security. Provide an example of each. (**3 Marks**)

QUESTION THREE (15 MARKS)

a) Compare and contrast symmetric key and asymmetric key cryptography in terms of their use in key distribution schemes. Provide examples of protocols that utilize each type. (**6 Marks**)

b) A Linux cloud server used by your team has the following discretionary access-control setup:

```
$ getent group admin users
admin:*:9001:alice
users:*:9002:alice,bobby,carla
$ ls -ld . * */*
drwxr-xr-x  3 carla users     4096 Apr  2  2017 .
-rwsr--r-x  1 bobby admin   241859 Jan  1  2013 proedit
-r--rw--w-  1 bobby admin     6355 Jul 24  2016 readme.txt
-rw--- r--  1 carla admin     1459 Jun 12  2016 runtime.cfg
dr--r-xr-x  2 bobby users     4096 Jul 23  2016 src
-rw-r--r--  1 bobby users    26339 Apr 28  2018 src/code.c
-r--rw----  1 alice admin     6701 Jan 23  2017 src/code.h
```

The file proedit is a normal text editor, which allows its users to open, edit, save and execute files. Copy and complete the access-control matrix illustrated below, such that it shows for each of the above five files, whether alice, bobby, or carla are able to obtain,

directly or indirectly, read (R) or replace (W) access to its contents. Underline any access that can only be obtained through elevated rights.

	proedit	readme.txt	runtime.cfg	src/code.c	src/code.h
alice					
bobby					
carla					

(**9 marks**)

QUESTION FOUR (15 MARKS)

a) Your colleague wants to use a secure one-way hash function *h* in order to store *h*(password) as password-verification information in a user database for which confidentiality might become compromised. For *h*, she suggests to use an existing CBC-MAC routine based on AES with all bits of the initial vector and the 128-bit AES key set to zero. Is this construct a suitable one-way hash function for this application? Explain why. (**7 marks**)

b) Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.

(i) Name *two* reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. (**4 marks**)

(ii) Outline a protocol for protecting the integrity and authenticity of Alice's messages to Bob that combines the benefits of a public-key infrastructure with those of using a message authentication code. (**4 marks**)

QUESTION FIVE (15 MARKS)

a) Kerberos involves three two-message exchanges, one between the client and the *Key Distribution Center (KDC),* one between the client and the *Ticket Granting Service (TGS),* and one between the client and the *server (S)* chosen by the client.

In Kerberos v4, the initial communication between the client *C* and the KDC *D* goes like this:

1. *C* sends a ticket request containing *C*'s name and a TGS's name *T*.
2. The KDC checks that both *C* and *T* are known to the system.
3. The KDC creates a ticket containing *C*'s and *T* 's names, *C*'s network address, the current time, the lifetime of the ticket, and a session key K_{CT}. This ticket is encrypted with *T* 's secret key K_{DT} known to both the key-distribution center *D* and the ticket-granting service *T*.
4. The reply to *C* consists of the ticket just described, *T* 's name, the current time, the lifetime of the ticket, and the session key, all encrypted with *C*'s secret key K_C. To keep messages that are intended for one purpose from being mistakenly used for another, the plaintext of the encrypted reply contains a constant string "krbtgt" identifying this as a ticket-granting ticket.
5. The client decrypts the reply and saves the ticket for use

(i) Explain briefly, in general terms, the purpose of the each of the three exchanges (between the client and KDC, client and TGS, and client and S. (**5 marks**)

(ii) Assume that the user's password is not stored on the client machine, and the client's key K_C is computed from the user's password by a known function. Why is Kerberos more convenient, for the human user, than a system in which the TGS is eliminated, and the client makes a Kerberos-style request to the KDC for each server connection? **(2 marks)**

(iii) In Kerberos v4, it is possible for an attacker to request a ticket for *C*, or simply overhear a request and response for *C*. Explain how this allows an attacker to do an offline dictionary attack. (**2 marks**)

(iv) In Kerberos v5, a *nonce,* or random number, is added to the client's request to the KDC, and included (as part of the encrypted response) in the reply from the KDC. Nonces are similarly used in the request and response from the TGS. What purpose does this serve? (**3 marks**)

(v) A Kerberos *realm* consists of a KDC, a TGS, a number of clients sharing keys with the KDC, and a number of application servers sharing keys with the TGS. In cross-realm authentication, a client in one realm wishes to use a server in another realm. Explain briefly how Kerberos is used in cross-realm authentication (across two realms) and state what key(s) must be shared between the two realms. (**3 marks**)