UNIVERSITY OF NAIROBI

SECOND SEMESTER EXAMINATIONS 2023/2024
THIRD YEAR EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

CSC411: Computer Networks Security

Date: 3rd June, 2024 **Time: 11:00Hrs – 13:00Hrs**

Instructions: Answer Question ONE and Two any other questions.

Question ONE (20 Marks, Compulsory)

a) Define the term ***principal*** and explain the meaning of ***identity*** in the context of computer security. (5 Marks)

b) Explain what is meant by a malware and describe at least four classes of malwares using appropriate examples where possible. (5 Marks).

c) Explain what is meant by One Time Password (OTP) authentication schemes and describe the potential vulnerability in utilizing them for authentication. Suggest another authentication scheme that can be used to augment OTPs in order to mitigate against the mentioned vulnerability, clearly outlining how the mitigation will be achieved. (5 Marks)

d) Use an appropriate example to illustrate how public key cryptography may be used for authentication purposes. State an important pre-condition that will be required in order for this authentication scheme to work. (5 Marks)

Question Two (15 Minutes)

a) In "Communication Theory of Secrecy Systems", Shannon proposed that security of cipher systems is measured using two concepts of unicity distance and cover time. Explain the meaning of each of these terms and how they are used to provide an indication of the security

of a cipher system. Further explain what theoretical concept has now superseded the notion of cover time in cryptanalysis. (6 Marks)

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

```
$ getent group admin users
admin:*:9001:anne
users:*:9002:anne,benson,caren
$ ls -ld . * */*
drwxr-xr-x 3 caren users 4096 Apr 2 2023 .
-rwsr--r-x 1 benson admin 241859 Jan 1 2018 simpledit
-r--rw--w- 1 benson admin 6355 Jul 24 2022 readme.txt
-rw----r-- 1 caren admin 1459 Jun 12 2022 runtime.cfg
dr--r-xr-x 2 benson users 4096 Jul 23 2022 src
-rw-r--r-- 1 benson users 26339 Apr 28 2024 src/code.c
-r--rw---- 1 anne admin 6701 Jan 23 2023 src/code.h
```

The file simpledit is a normal text editor, which allows its users to open, edit, save and execute files. Taking the set of objects to be files only (not directories) and using only the subjects provided above, construct an Access Control Matrix (ACM) such that it shows for each of the above five objects whether the subjects 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. (9 Marks)

Question Three (15 Minutes)

Consider the case of Mirai botnet attack of September 2016 that was presented in class. Mirai is a Japanese word that means "the future". However in this context, Mirai refers to a malware that infects IoT devices that run on ARC processors. It turns them into a network of remotely controlled bots or "zombies". A network of bots is often referred to as a botnet and is often used to launch DDoS attacks.

a) Describe in details how the Mirai botnet works (3 Marks).
b) Give a justification for the use of the name "Mirai" for this botnet and one reason why Mirai is still considered as one of the most dangerous threats on the Internet today. (2 Marks)
c) Other than PureMasuta and OMG, describe two other variants of Mirai botnet. (2 Marks)

d) Explain why PureMasuta and OMG are considered as an open source weapons. (2 Marks)

e) Describe two different models that can be employed to launch botnet attacks such as Mirai. (4 Marks)

f) Explain the connection between Mirai and click fraud attacks. (2 Marks)

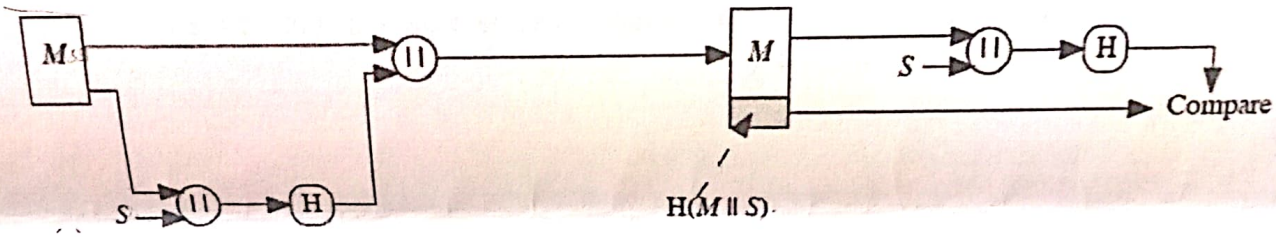
Question Four (15 Minutes)

a) Describe the one-way property of hash functions. (2 Marks)

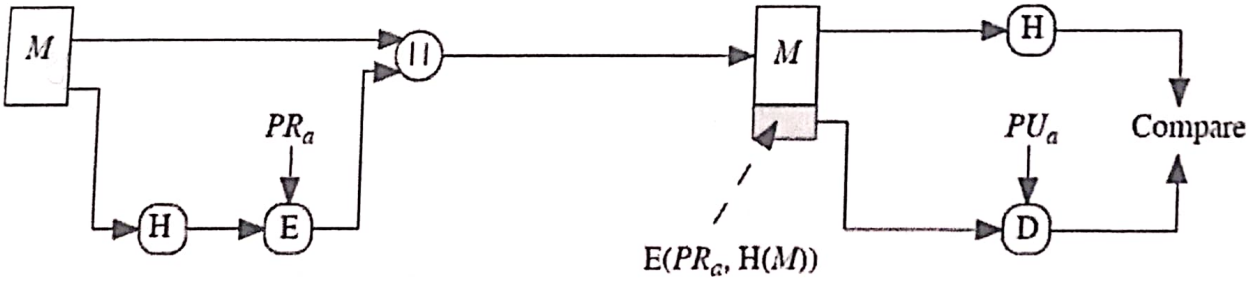
b) Describe the weak collision resistance property of hash functions. (2 Marks)

c) Describe the strong collision resistance property of hash functions. (2 Marks)

d) The following figure shows a technique for authentication. M is a message and S is a shared secret. Explain the problem in this scheme if the hash function does not have the one-way property (that is, what could a malicious user do and how could they do it?) (2 Marks)



e) *The following figure shows a technique for authentication. M is a message sent by node a. Explain the problem in this scheme if the hash function does not have the weak collision resistance property (that is, what could a malicious user do and how could they do it?). (2 Marks)*



f) User A wants to digitally sign a document M and send it to B. Give a function that describes how the signing is performed (you must also describe all variables used) and explain what is sent from A to B. (2 Marks)

g) User A wants to send a MAC authenticated message M to B. Give a function that describes how the authentication data is generated (you must also describe all variables used) and explain what is sent from A to B. (2 Marks)

h) Explain why MAC-based authentication cannot be used as a digital signature. (1 Mark)

Question Five (15 Minutes)

In July 2023, there was a massive Distributed Denial of Service (DDoS) attack against e-citizen, the Government of Kenya's service delivery platform. A network of compromised computers (botnets) was used to generate traffic that the platform was not able to handle. You have been contracted to advise the government on fault tolerance mechanisms that they need to put in place to enhance resilience of this platform against such attacks in the future. Using appropriate examples where necessary, describe in details FIVE strategies that you will recommend for adoption by the government in order for them to achieve the stated objective.