CPR E 431: INFO SYSTEM SECURITY
Midterm Exam: SAMPLE
Time Allowed: 50 minutes
This sample midterm exam gives you the layout of the exam and possible exam problems/questions. The actual exam may have more/fewer questions/sub-questions.

1. Choose/circle the right answer

i. The primary purpose of an IDS is to detect intrusions, log suspicious events, and send alerts.

a- True b- False

ii. An ABAC model can define authorizations that express conditions on properties of both the resource and the subject.

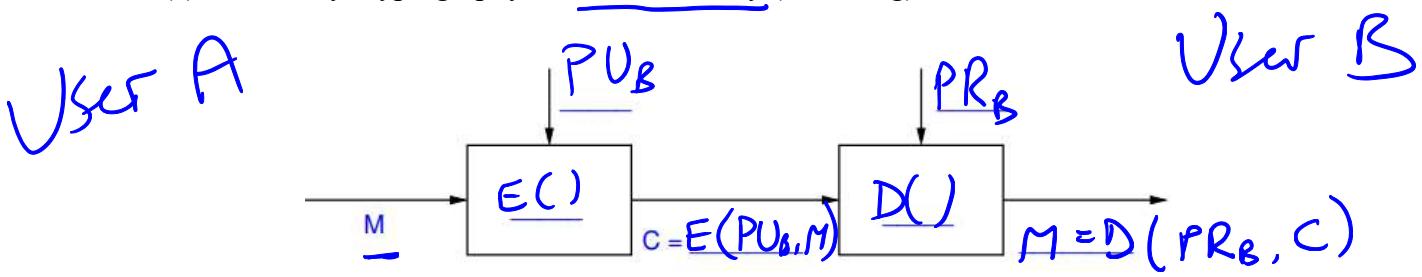
a- True b- False

iii. _____ is a virus that can rewrite itself completely after each iteration/execution.

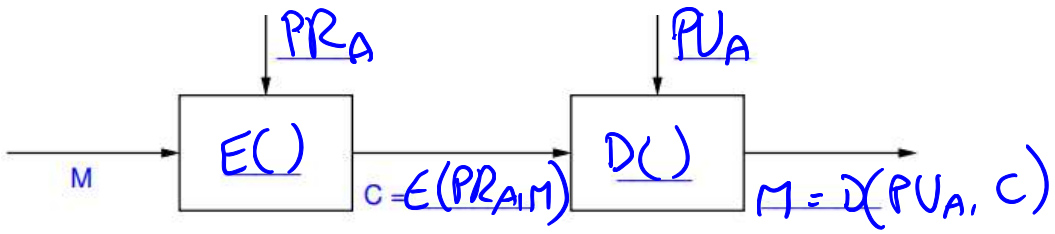
a- Stealth Virus b- Polymorphic Virus
c- Metamorphic Virus d- Encrypted Virus

2. The following three figures show models for different cryptographic operations, with user A on the left and user B on the right. Using the notation used in lectures (and given in some parts of the figures), fill in the missing information on the blank lines.

(a) Public key cryptography for confidentiality (6 missing)



(b) Public key cryptography for authentication (6 missing)



(c) Write an equation that shows how user A creates a signature of a message M that it wants to send to B

Digital signature

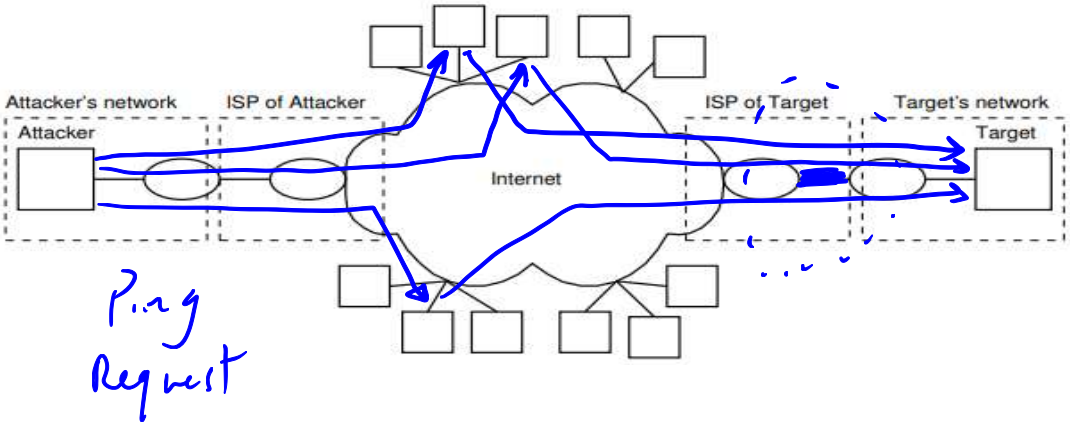
$$S = E_{RSA}(PR_A, H(M))$$

$$= E_{RSA}(PR_A, M \| H(M))$$

3. The following questions provide a template network diagram and require you to describe the directions of the arrows that may be drawn on this figure to show the flow of packets in the attack mentioned. Please be specific in your description (for example one arrow or multiple arrows sent from the attacker to the intermediate hosts or from the attacker to the tartget). In your description, give the name or type of message/packet being sent.

Unless otherwise stated, assume the link from the ISP router to the target router is the bottleneck link, hosts on the Internet are not under the control of the attacker, the ISP of the attacker does not filter packets with fake addresses, and the attacker does not use a fake address.

⇨ Describe a Ping flooding attack, where the attacker uses fake source addresses and reflectors.



4. For each of the following vulnerabilities of passwords, explain one countermeasure, and explain one drawback of that countermeasure.

(a) Specific account attack, where an attacker submits password guesses on a specific user account.

→ Limit wrong password trials to 3- attempts

→ Attacker can change the device/IP to gain new attempts.

(b) Computer hijacking, where an attacker gains access to a computer that a user is currently logged in to.

→ Auto- log-out after a certain amount of time

→ Attacker gain access before the auto-log-out take place.

(c) Popular password attack, where an attacker tries a popular password with many different user IDs.

→ If the same device/IP is trying to access the system using different user IDs then the system should block his device/IP.

→ Attacker may use a different Computer/IP

5. The following shows the partial output of the /etc/shadow file on a Linux operating system. This file store the usernames and password related information for users of the computer. The values are separated by a : character. (Note that the data for each user is normally on a single line; I have wrapped it across two lines to fit within the page for this question).

```
$5$8MlKVqhP$sdf897ds12poheds9032.asjfeiojfsdf9REWk32ds/
```

(a) Can you tell the length of the original password of this hash? (Yes/No) Explain your answer.

No. Based on the hashing process, any password with any length will produce a fixed-length hash.

(b) For the hash above, what is the hash algorithm used? What is the salt value assigned to this user?

Hash Algorithm (number or name): 5 SHA-256

Salt Value: 8M1KVqhP

6. Answer the following questions:

(a) Mention one difference between a worm and a virus.

Virus	Worm
Must have a host to propagate	A host is not required
Must be triggered	No trigger needed

(b) Briefly explain the differences between discretionary, role-based, and mandatory access control.

slides

(c) Briefly explain the differences between Masquerader, Misfeasor, and Clandestine intruders.

outside insider insider or outsider Admin

(d) Briefly explain the main difference between Anomaly IDS and Signature IDS.

Signature IDS Compares the behavior of any program/packet with Pre-Configured/Pre-determined Patterns (signature)

Anomaly IDS It is capable of alerting on unknown suspicious behavior. It may use Machine learning to train the system with normal baselines.