# Sample Midterm

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**P**oints: \_\_\_\_\_\_\_\_\_\_\_/**100**

1. **(3 pts)** Define what is vulnerability and what is exploit. What effect can exploit have on a system?

Vulnerability = bug in the code

Exploit = input to the code that exercises the vulnerability

Effect = any unwanted behavior (**intrusion**, 1 out of = crashing the machine, slowing down the machine)

1. **(5 pts)** Explain what is tragedy of commons. Why do we say that most problems in cyber security suffer from tragedy of commons phenomenon?

Tragedy of commons = there’s a common resource, everyone benefits from using it but if someone overuses it everyone is hurt. Internet is a shared resource, in many cases our security depends on security of others, and for many problems a defense needs to be deployed at a point that does not see a direct benefit.

1. **(4 pts)** Describe how a homophonic cipher works. Then describe how a polymorphic (polyalphabetic) cipher works.

Homophonic cipher maps each character to a set of symbols. Size of the set depends on the frequency of characters in plaintext = more frequent are mapped to a larger set. One character from the set is chosen at random during encryption. Number of symbols in output alphabet is greater than those in input alphabet.

Polyalphabetic cipher uses multiple mappings, one for each character, it cycles back when it runs out of mappings.

1. **(10 pts)** Define what is a block cipher and what is a stream cipher. What modes of operation exist for a block cipher (it is enough to just list the modes).

* Stream cipher operates bit by bit (or byte by byte) – encryption is simple operation, strength is in long and non-repeatable key
* Block cipher operates on fixed-size blocks – encryption is complex operation, key is usually the size of a block
* Block cipher can work in ECB, CFC, CFB or OFB mode

1. **(10 pts)** Explain how linear feedback shift registers work

LFSRs (are used for random number generation) – number of bits in a register, each step shifts bits to one side, a new bit is generated by combining the contents of register and the result is put at the gap. There’s a tap sequence that determines which bits are combined (XORed).

1. **(8 pts)** Alice wants to send message M to Bob. How can she ensure the following properties, using asymmetric cryptography:
   1. **(2 pts)** Confidentiality

Encrypt with Bob’s public key

* 1. **(2 pts)** Integrity but not confidentiality

Encrypt with Alice’s private key – hash first then encrypt

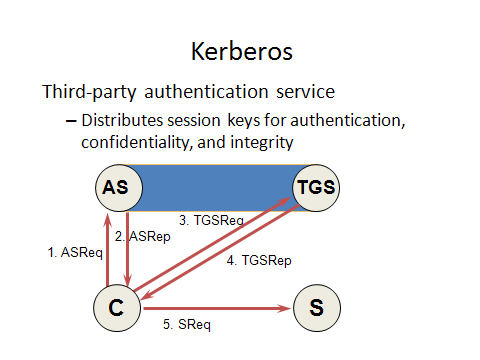
* 1. **(2 pts)** Confidentiality and integrity

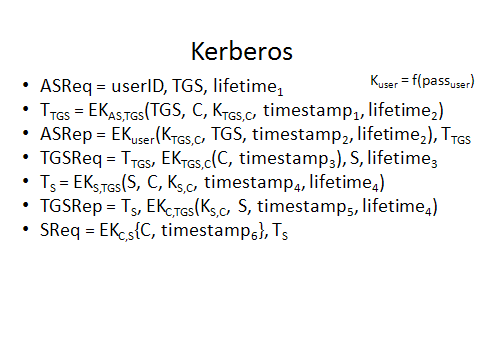
Hash M, encrypt with Alice’s private key for integrity, Encrypt M with Bob’s public key for confidentiality

* 1. **(2 pts)** Confidentiality, integrity and non-repudiation

Same way as in c.

1. **(10 pts)** Describe how Kerberos works. Make sure to show all the steps needed for a client to access a server.





1. **(10 pts)** Explain how cookies can be used for authentication. What are the advantages and disadvantages of such authentication approach?
2. Client requests a service
3. Server asks for username/pass
4. Server gives client a cookie. Cookie has any of: username and pass, session ID, extra info about session = need some way to ID user and session from cookie – cookie should be unforgeable
5. Client gives server this cookie each next time, no user/pass
6. When client logs out cookie is deleted and server closes this session

Advantages: Easy for user

Disadvantages: Cookies can be stolen from machine or in transit

1. **(10 pts)** Our company is implementing Bell-Lapadula model for access control. Below are the access control matrix and the classifications of various objects and people. After going through them answer the following questions. Make sure to show the decision process that lead to your answer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bob | Chris | Amy | Laura |
| Salaries | write, read |  | write, read | read |
| Vacations |  | write, read |  |  |
| Building map | read | read | read | write, read |
| Orientation | read | read | write, read |  |

Salaries is a top-secret file

Vacations is a secret file

Building map and Orientation are unclassified

Bob and Chris have secret clearance

Amy has top-secret clearance

Laura has confidential clearance

* 1. **(2.5 pts)** Which files can Bob read?

Bob can read building map, orientation and vacations based on his clearance level but ACM only gives him read access to building map and orientation. Bob can write a secret and top-secret level and he has write access to salaries from ACM.

* 1. **(2.5 pts)** Who can read Building map?

Based on classification anyone can read. ACM also gives all four access to read.

* 1. **(2.5 pts)** Who can write Vacations file?

Based on classification Bob, Chris and Laura could write. Based on ACM only Chris can write.

* 1. **(2.5 pts)** How can we grant to Laura permission to read the Vacations file?

She needs to be given secret clearance and read access in ACM

1. **(10 pts)** What kind of traffic would attacker need to generate to learn:
   1. **(2 pts)** All the DNS information about a network

DNS zone transfer with the DNS server of the network

* 1. **(2 pts)** Live machines within a network

Ping sweep (SYN sweep)

* 1. **(2 pts)** Services within a network

SYN sweep or UDP pkt to all ports on live machines

* 1. **(2 pts)** Vulnerabilities in installed applications within a network

Vulnerability scan

* 1. **(2 pts)** Network topology

Traceroute