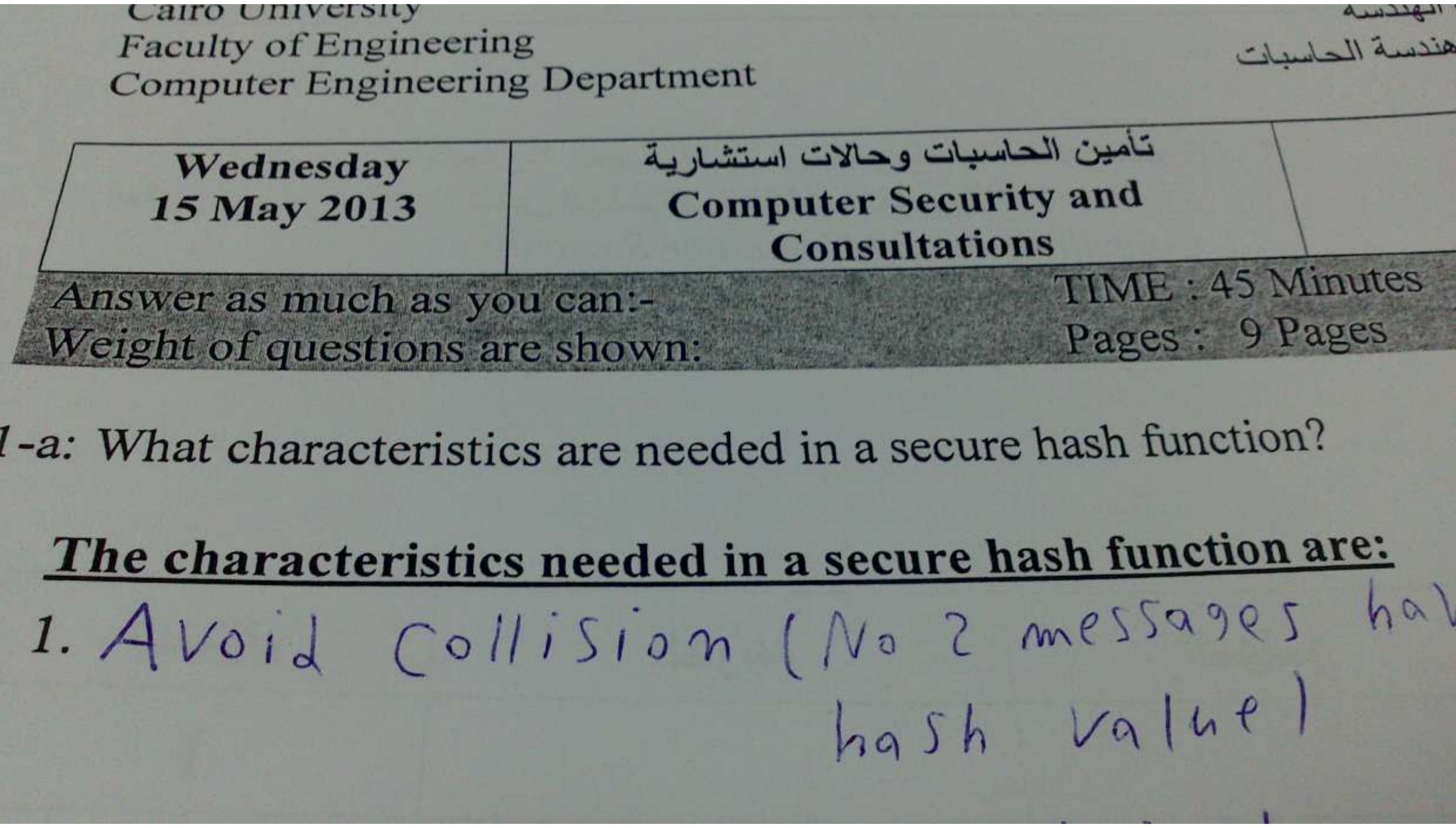


Cairo University
Faculty of Engineering
Computer Engineering Department

الهندسة
هندسة الحاسبات

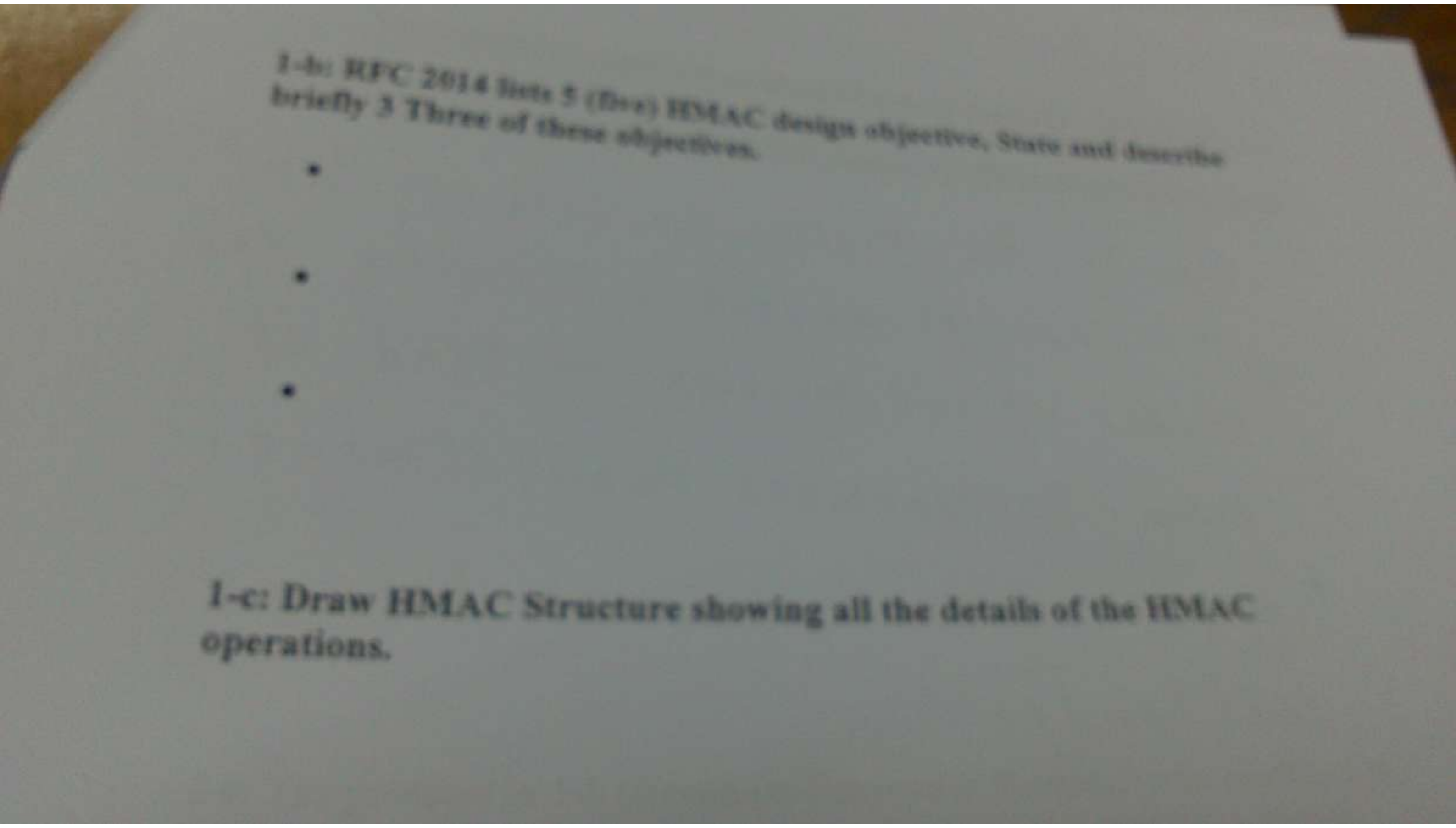
Wednesday **15 May 2013**	تأمين الحاسبات وحالات استشارية **Computer Security and Consultations**	

Answer as much as you can:- TIME : 45 Minutes
Weight of questions are shown: Pages : 9 Pages

1-a: What characteristics are needed in a secure hash function?

The characteristics needed in a secure hash function are:

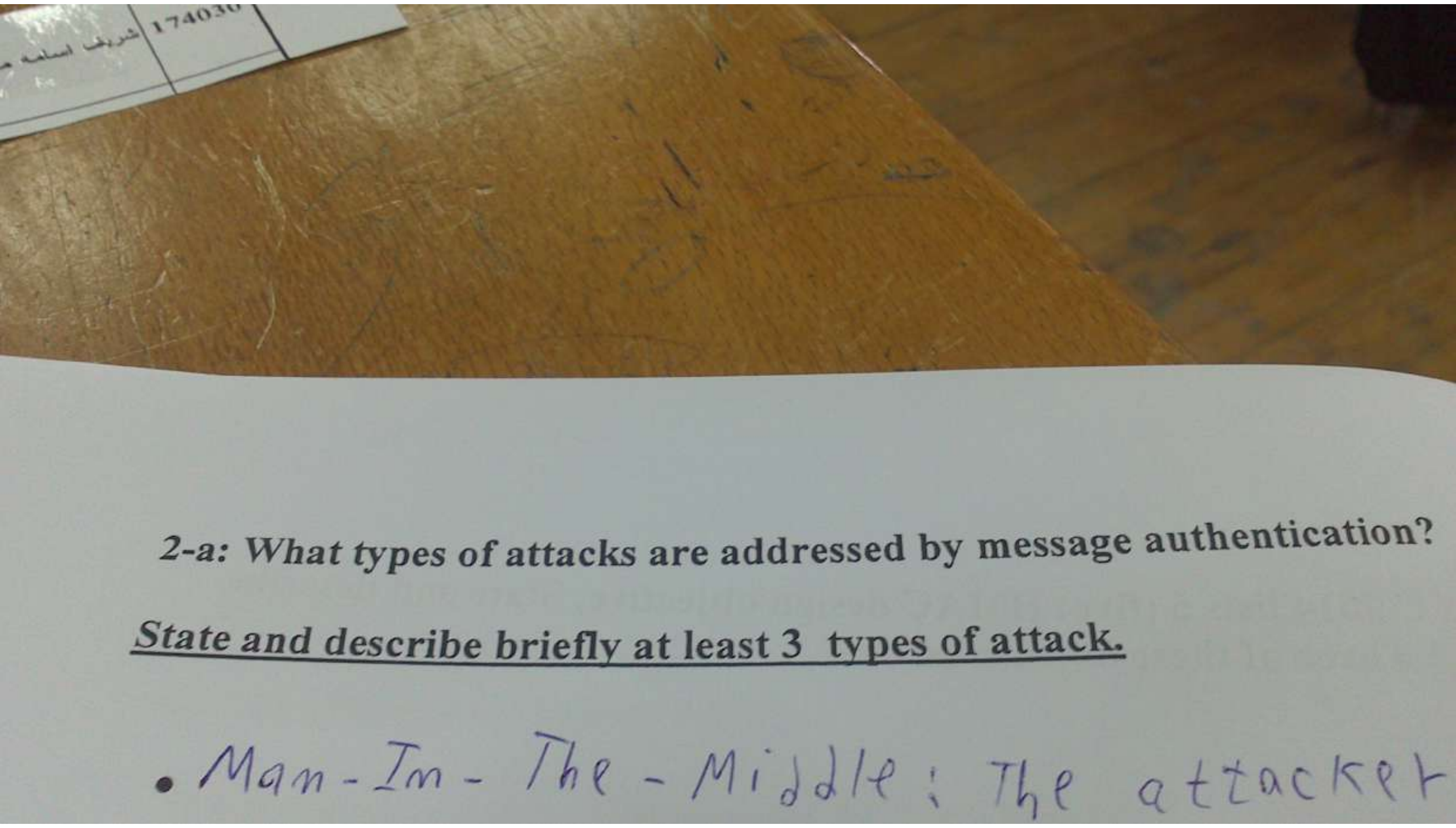
1. Avoid Collision (No 2 messages ha
hash value)



1-b: RFC 2014 lists 5 (five) HMAC design objective, State and describe briefly 3 Three of these objectives.

-
-
-

1-c: Draw HMAC Structure showing all the details of the HMAC operations.

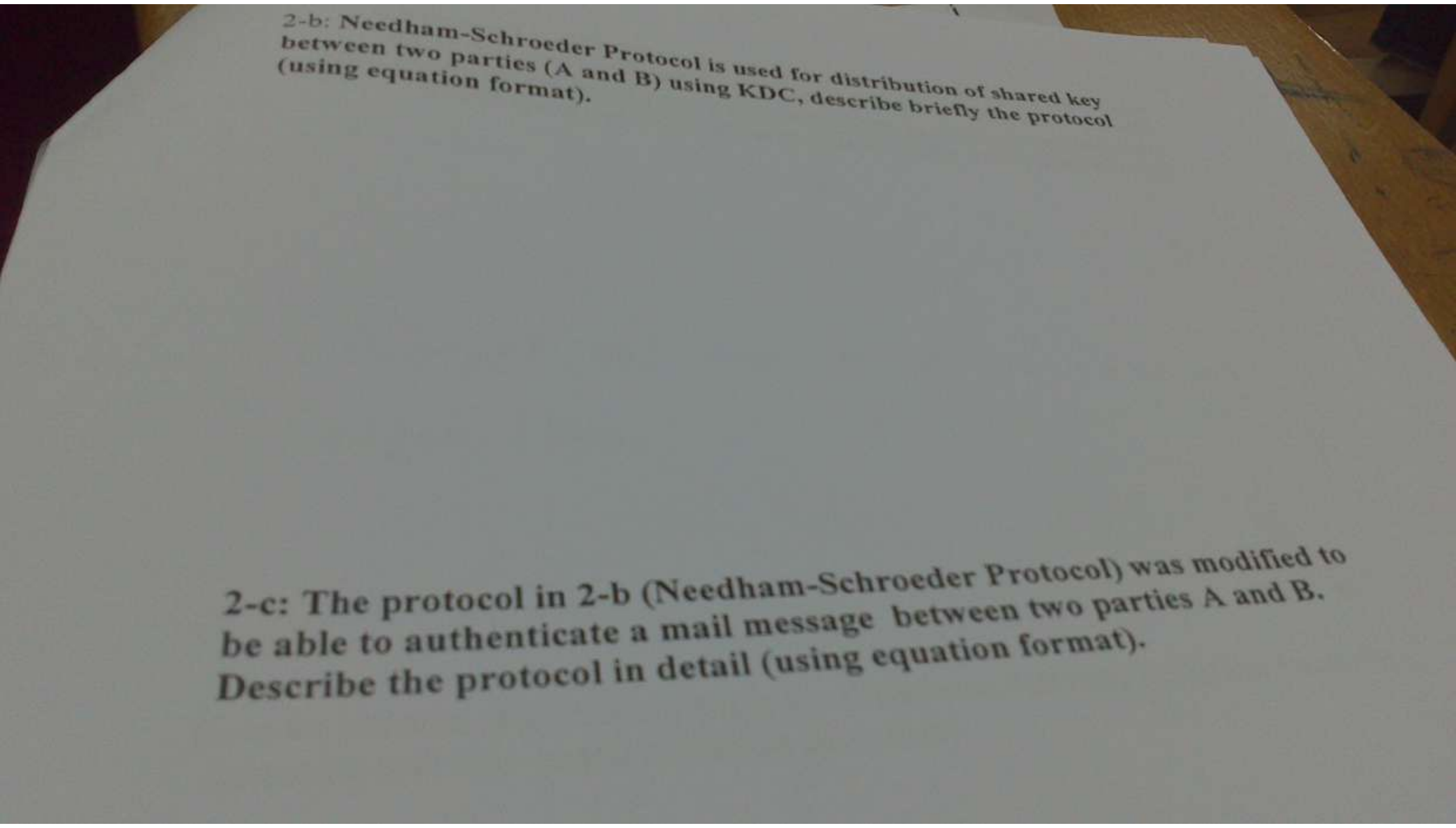


شريف اسامه 174030

2-a: What types of attacks are addressed by message authentication?

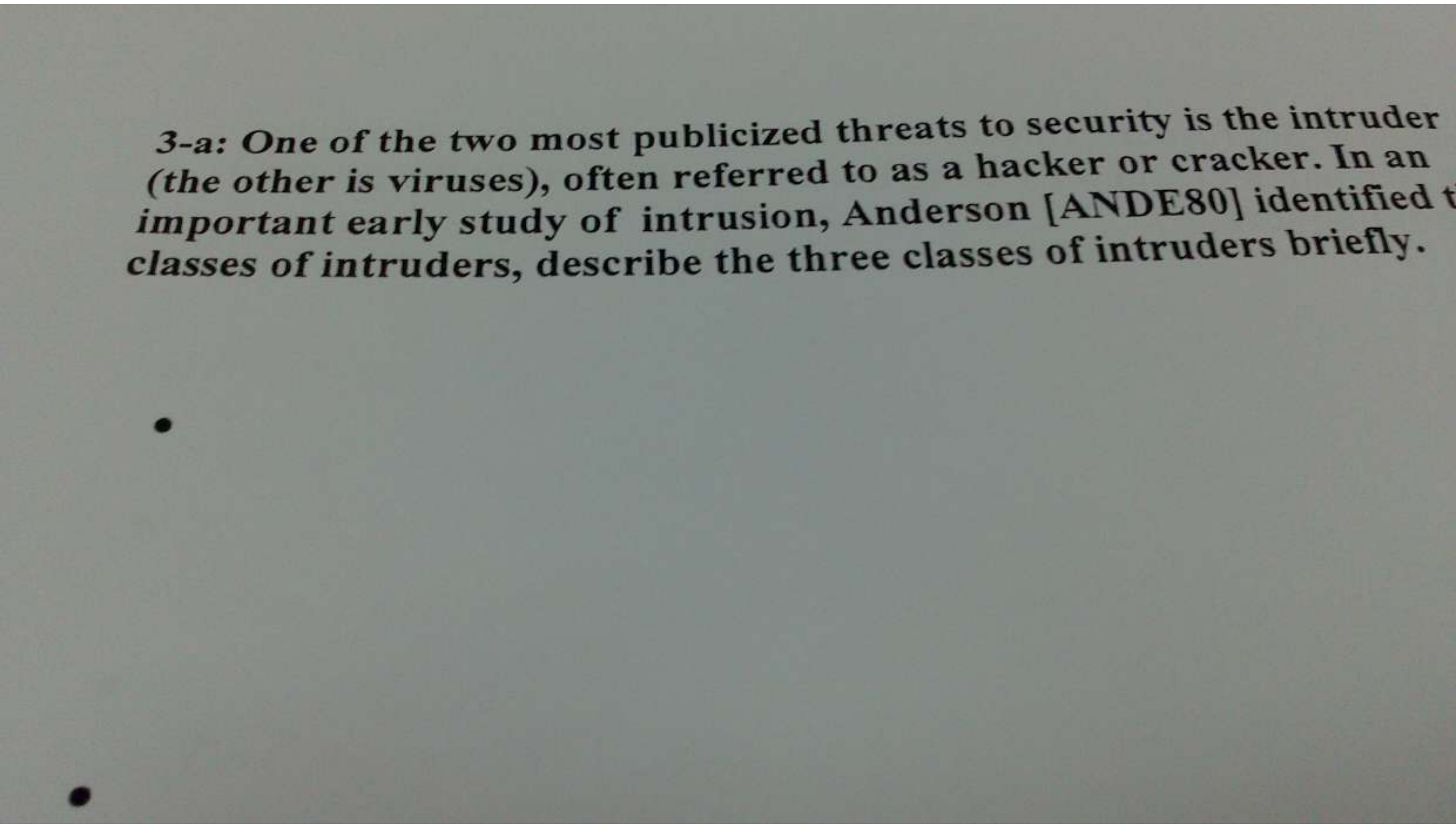
State and describe briefly at least 3 types of attack.

- Man-In-The-Middle: The attacker



2-b: Needham-Schroeder Protocol is used for distribution of shared key between two parties (A and B) using KDC, describe briefly the protocol (using equation format).

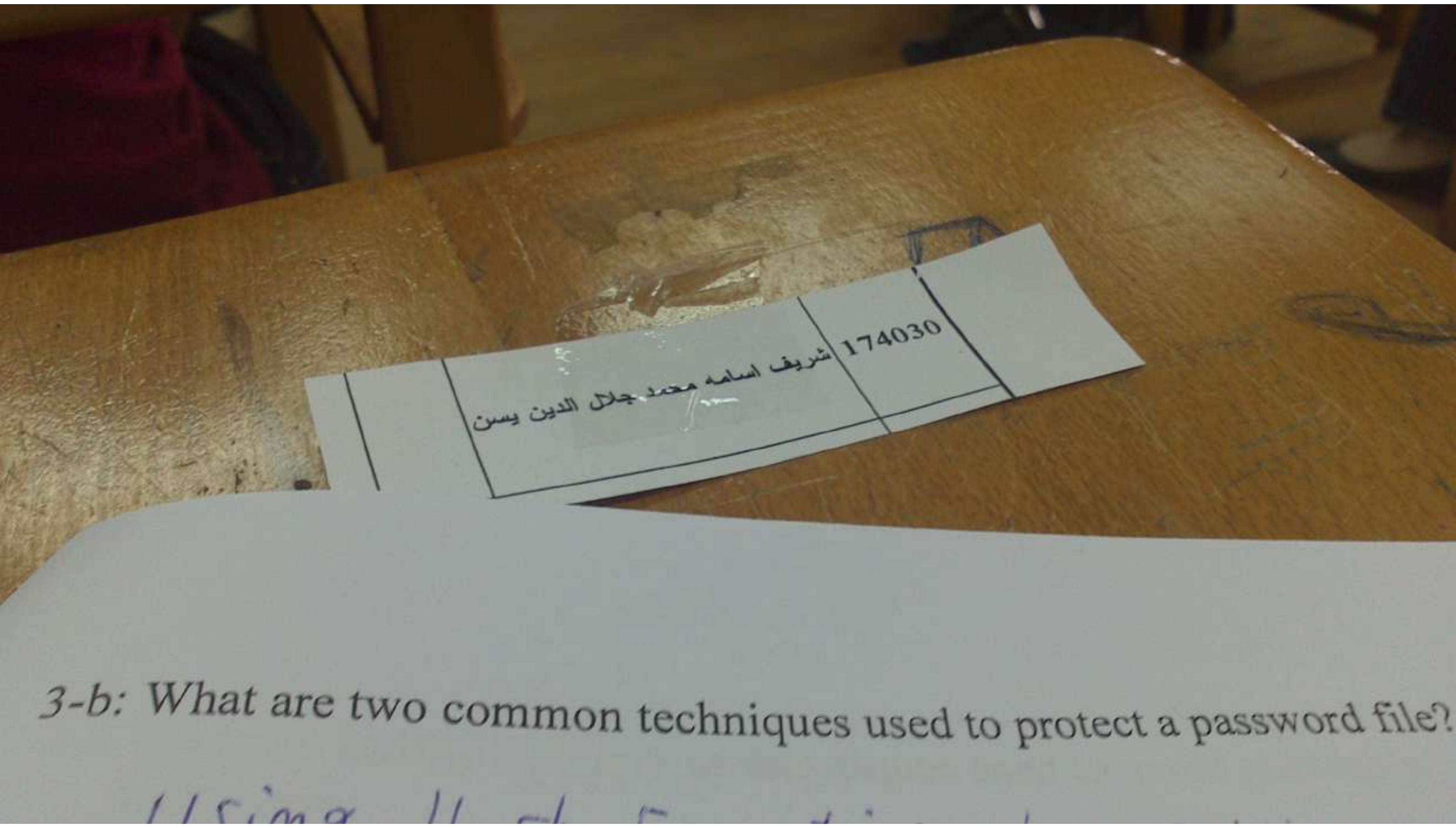
2-c: The protocol in 2-b (Needham-Schroeder Protocol) was modified to be able to authenticate a mail message between two parties A and B. Describe the protocol in detail (using equation format).



3-a: One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker. In an important early study of intrusion, Anderson [ANDE80] identified t classes of intruders, describe the three classes of intruders briefly.

•

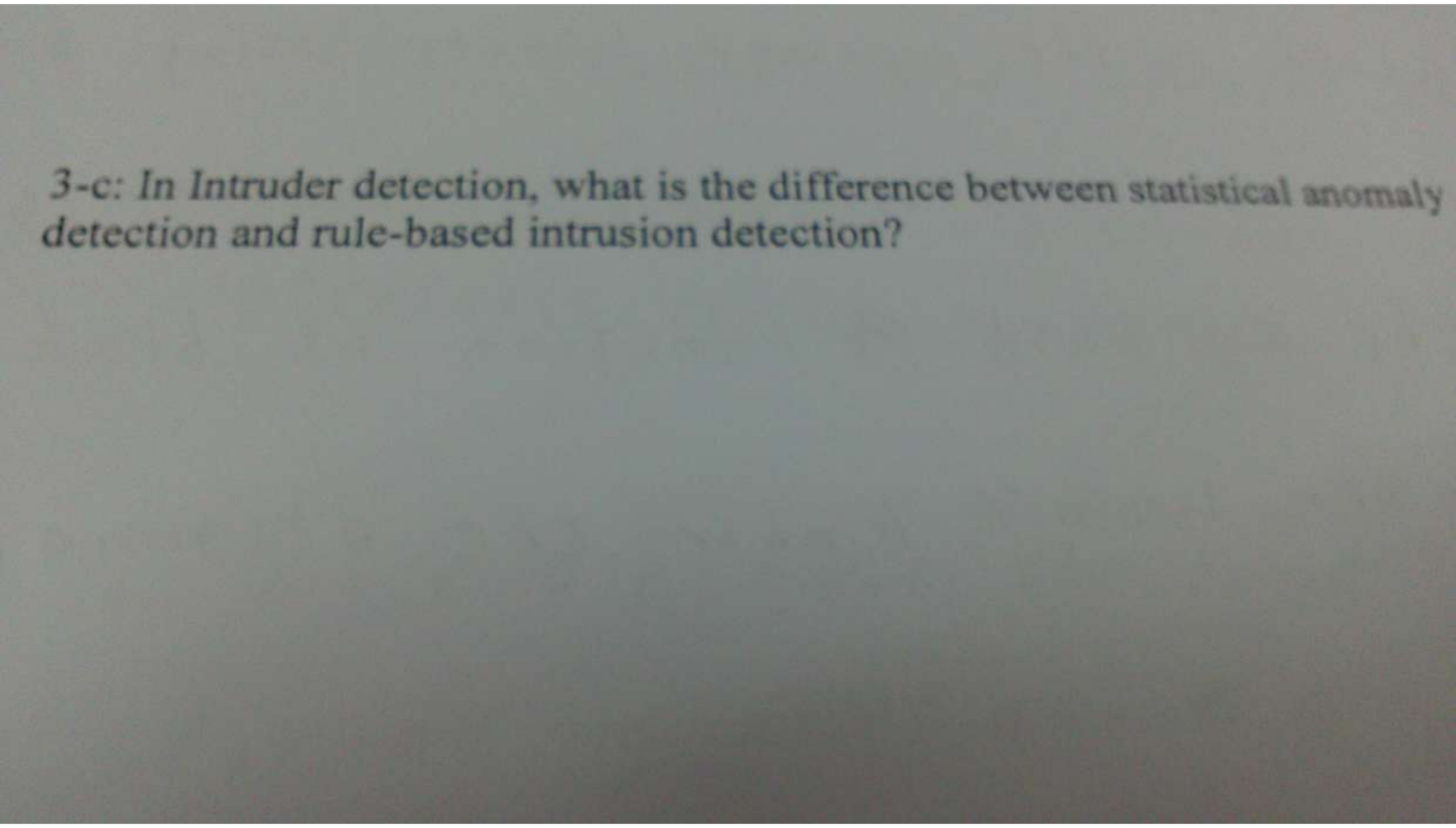
•



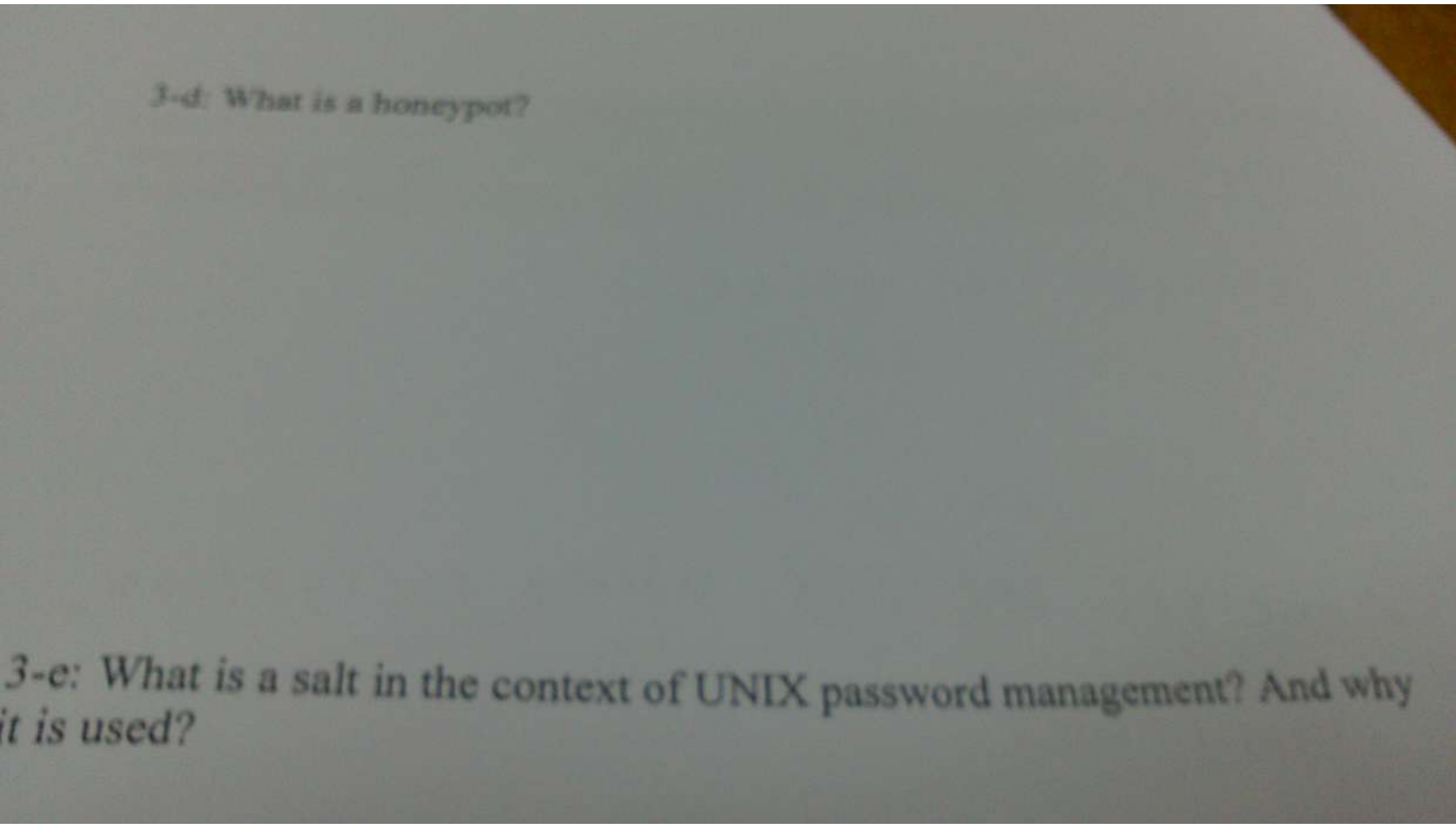
	174030	شريف اسامه محمد جلال الدين يسن	

3-b: What are two common techniques used to protect a password file?

Using Hash Function

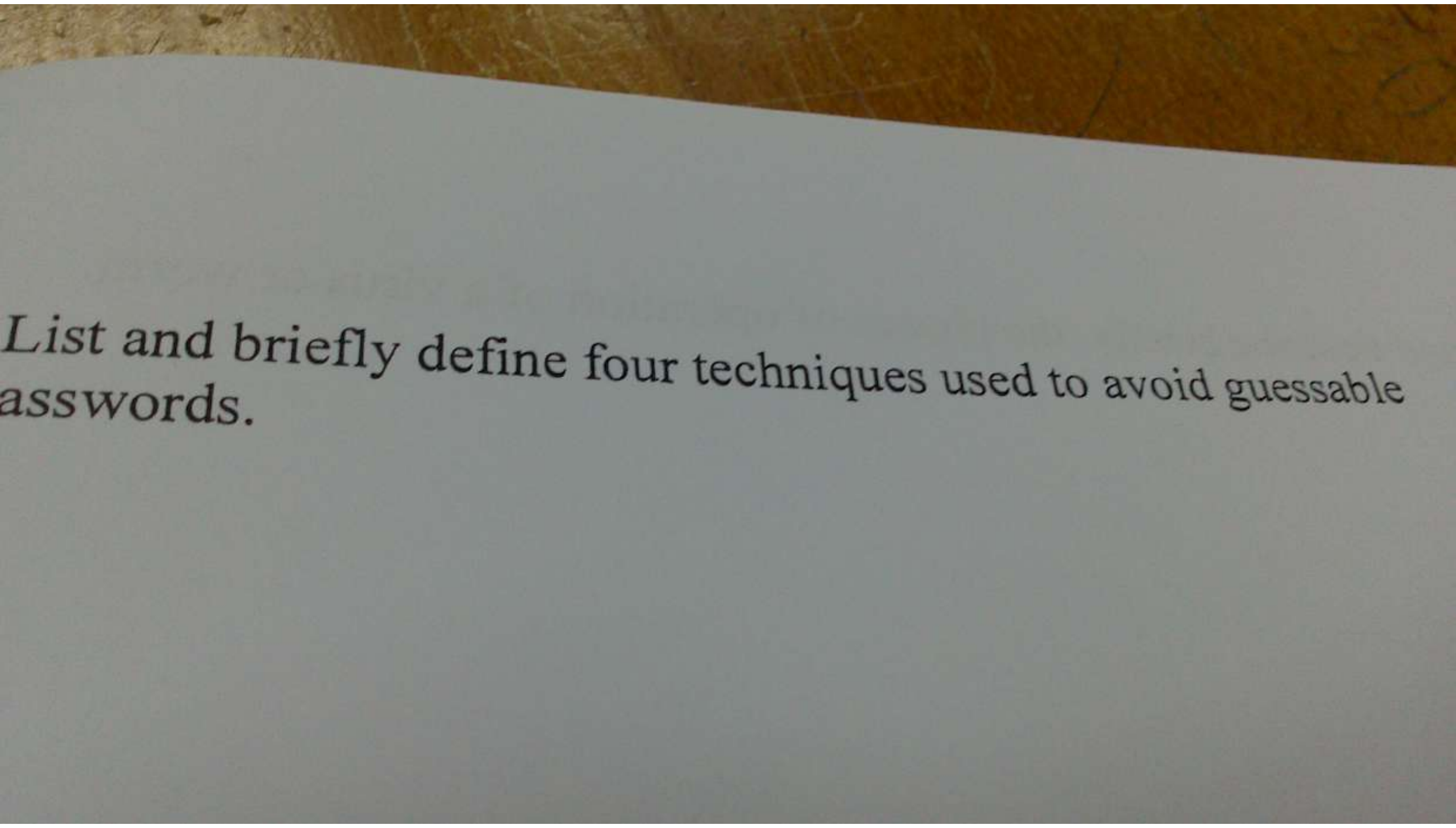


3-c: In Intruder detection, what is the difference between statistical anomaly detection and rule-based intrusion detection?

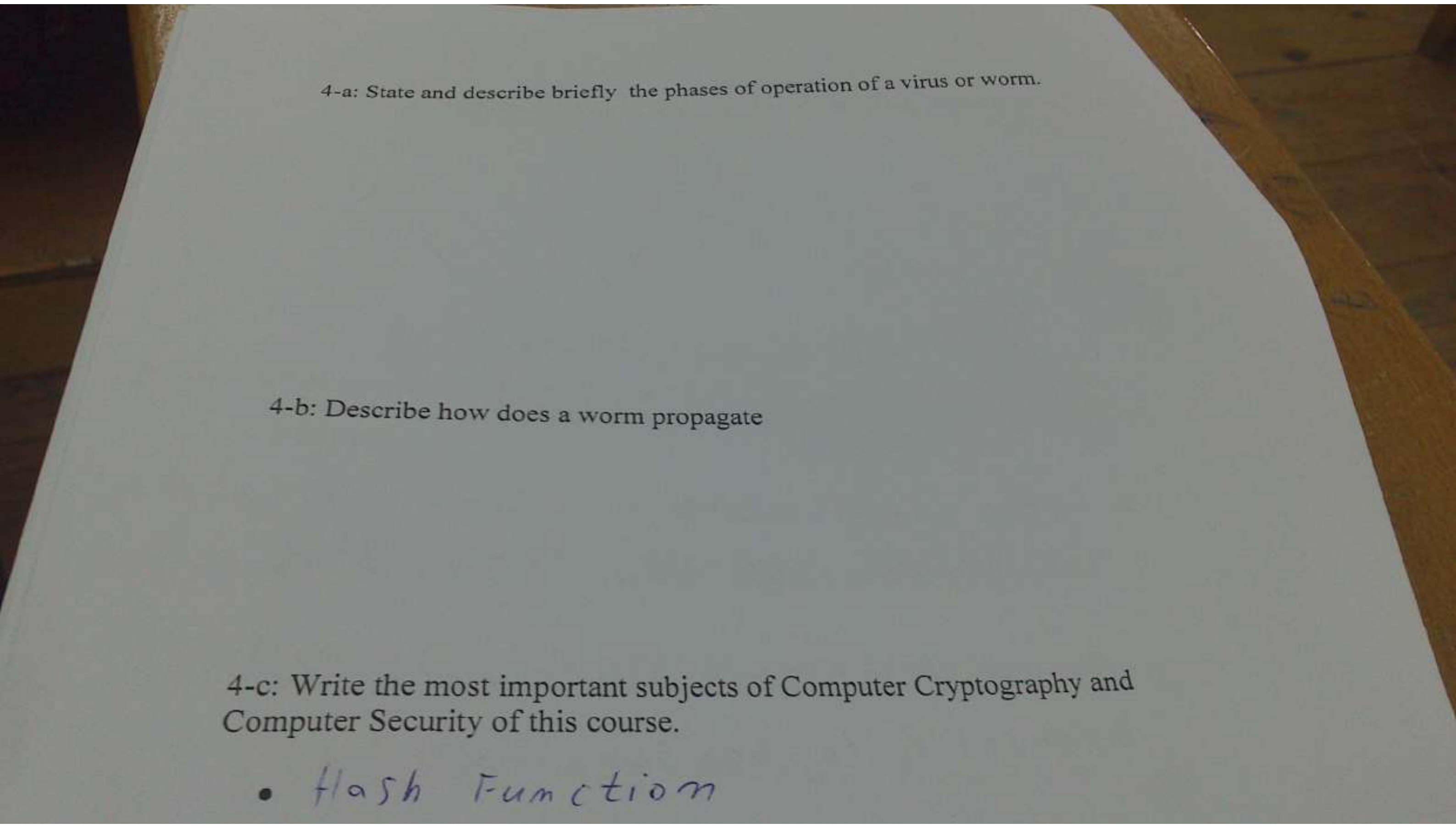


3-d: What is a honeypot?

3-e: What is a salt in the context of UNIX password management? And why it is used?



List and briefly define four techniques used to avoid guessable asswords.



4-a: State and describe briefly the phases of operation of a virus or worm.

4-b: Describe how does a worm propagate

4-c: Write the most important subjects of Computer Cryptography and Computer Security of this course.

- Hash Function