**Security**

Q1)

What is the Difference between :

1. **Qualitative and Quantitative risk**

Risk Analysis = Threats\*Vulnerability\*Asset

Measuring security

Quantity: number

Quality: scale or Range

1. **Universality and Distinctness biometric property**

**Universality** Each person should have the characteristic, Failure to Enroll Rate (FER)

 **Distinctness** Different persons should have different biometric properties, False Match Rate (FMR)

1. **Confusion and diffusion in cryptology**

confusion“ standing for substitution operations and

„diffusion“ standing for transposition or permutation operations.

1. **Distributed denial of service and Denial of service**

In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server’s bandwidth and resources.

[DDoS attack](https://www.incapsula.com/ddos/ddos-attacks/), uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet. A DDoS attack is, therefore, much harder to deflect, simply because there is no single attacker to defend from, as the targeted resource will be flooded with requests from many hundreds and thousands of multiple sources.

1. **Virus and warm**

لوورمز هي برامج بتنتقل عبر النتوورك الهدف منهم عملية نقل الملفات الضارة، وكأنها شاحنة بتنقل الفايروسات والانتروجنز،
اما الزومبي هي عبارة عن اجهزة كمبيوتر فيها ثغرات او vulnerability معينة بحيث انها بتيح استغلالها من قبل الـ attacker عشان مثلا يخفي نفسو (يبين الهجوم من هذا الجهاز) او انو يجندو عشان يستغلو في DDos

1. **Symmetric and asymmetric cipher ??** Symmetric algorithms: the same key is used for encryption and decryption .Asymmetric algorithms: different keys are used for encryption and decryption.

Q2)

 Password Question ( so2al i7temalat zai ile ija bel midterm o el assignment)

 O so2al entropy sahel

 **O so2al 3n el biometrics ino jeeb 4 biometric properties 2 physiology and 2 behavioral and give one advantage and one disadvantage for each and one application method on each one**

1. Universality
2. Distinctiveness
3. Permanence
4. Collectability

Physiological:

Physical features ”unchangeably” attached to a person

E.g. fingerprint, DNA, and face

Behavioural:

Behaviour that is very specific to a person

E.g. signature, gait, and voice

Advantages: Easy to use, portable

Disadvantages: Expensive, replay attacks may be possible, privacy issues, characteristics can (in general) not be changed, characteristics can be injured, intrusive

**O ish 6areqten to be strong but still easy to remember password**

pick two random words, add a hyphen, and tack a number on the end.

 A space can count as a special character.  That way you have a password that uses all of the rules and is still easy to remember.

Q3)

 Transportation cryptology

1. Find the cipher text
2. How we can make it harder to attacks?
3. What is the number of possible keys
4. Prove that decryption is the inverse of the encryption (a5o o5tak iza bt7ilo :P)

O fe so2al DES ta6beeq mobasher bs ma 7aleto 3shan ma kont darsa el DES :P

**Ish elfarq been el monoalphabetic wel polyalphabtic o ish eladvantages ll polyalphabtic over el molealphabtic**

Effectively smears the characteristic statistics of natural language text.For a long time was thought to be unbreakable.

 Q4)

1. **The difference between misuse and anomaly appropriate with IDS, which is the best and why?**

Misuse detection involves gathering information about indicators of intrusion in a database and then determining whether such indicators can be found in incoming data.

Anomaly detection involves a process of establishing profiles of normal user behaviour, comparing actual user behaviour to those profiles, and alerting if deviations from the normal behaviour are detected.

misuse because it can recognize new attack forms from old attacks (existing knowledge) but ther is trade off on false positive and false negative

1. **What is the architecture of the snort …?**

****

1. **Given the message and the http … write the rule of the snort..?**
2. **The difference between false negative and false positive and which is more dangerous**?
3. البوستف منع اشي مش لازم يمنعو النيكاتف انو الي معو باكيت عادي اعتبرها صح
4. وانو النيكاتف اخطر
5. **What are the matrices of anomaly detection of intrusion?**

Metrics - measures of particular aspects of user behaviour. Each metric is associated with a threshold or a range of values.

 Q5)

1. Given the code (the same on the slides) draw the stack and what is the problem of this code?
2. **(About the SQL injection and what is the counter measures against it?)**

using validation methods on the input of user.

1. Given a database table write an Sql statement ……
2. O ishe so2al fee code o bdk t7aded iza virus wela l2 o ibsr sho
3. O rasmt el digital immune system m3 shwait share7