Questions from the first Oral Exam

1- What is a composition theorem? It's based on inequality…..

We extended composition theorem to computational theorem?
What is Asymptotic (version) formulation in composition theorem?
How many times do we use (m) in Asymptotic version in polynomial?
What type of distance is this? variational distance.
Can you describe the scheme protocols in 2G mobile?
What are the limitations of 2G? what kind of information
What is the secret key rate?

2- What is the best layer to apply a secret? Physical layer ?

Why is the physical layer the best?
Can you give an example why we use to protect application layer data.
What is a public key encryption?
What are the requirements for the public key?
How can we say k prime (public key) is compatible with one another?
What is a universal hashing function?
Why do we need universal hashing function? What is its purpose?
How does the handshake work in TLS? What is its purpose?

3- What is the difference between Digital signature and message authentication code?

What services do they provide?
What is the difference between source authentication messages?
What is the difference between message source authentication and entity source authentication?
What is the definition of perfect secrecy? Why is It independent?
What is a wiretap channel in physical layer?
How do we solve a problem in wiretap channel?
How do we order the channel?
How does McEliece Cryptosystem works in encryption?
How does Elgamal Cryptosystem work in encryption and in signature?
Is Elgamal probabilistic? Where does the probabilistic come from?

4- What is a secrecy key rate? See Last lecture?

Talk and explain memoryless channels, what results do we have?
Talk about secret key capacity.
What do we require in an entity authentication protocol? (correctness, security, non-transferability)
Give an example of an entity that does offer non-transferability and which doesn't.

5- Talk about integrity protection, what are the requirements for Symmetrics Encryption

In Digital signature using RSA, How to generate keys? What is needed for public and private keys? How to sing and verify messages? existential forgery!!!…….
…….

All the best AB.