- single round of DES
- diagram public key encryption to distribute symmetric secret key
- hash function requirements
- all message attacks + brief description of each attack and how to handle each one
- diagram of public key certificate
- public key certificate requirements
- objective of HMAC
- draw HMAC
- equations of Needham
- 5 modes + diagram of OFB + OFB adv & disadv
- is it possible to perform parallel block encryption using CBC mode , what about decryption?
- 3 classes of intruders
- RSA algorithm + mas2la
- DH algorithm + mas2la + man in the middle attack + is it possible to perform man in the middle attack with just one pair
- get multiplicative inverse arkam (nfs arkam final 2015 bs hwa fe final 2015 mtgaweb 3'lt)
- RSA chosen cipher text attack (mas2la shabaho kda htt3ml b nafs el tare2a)
- ssl record protocol eh hwa
- one field in ssl record protocol header
- draw ssl architecture
- choose 2 components of ssl architecture and write brief description
- https consists of .... and ....
- ssl alert protocol by3ml eh
- honeypot

Elkanon kan feeh so2al bthy2ly msh mtkkrar , bta3. El 5ashb da , el kan bys2l 3la 5tab eldaman