

- 1- Playfair cipher encrypt University using worldcup
- 2- Bob & Alice
- 3- Chapter 10 Public Key distribution using Authority
- 4- Chapter 9 , Securece & Authentication (A encrypts with PUB, PRA) ...
- 5- Chapter 10 , Deffie Hellman Algorithm , when it is used and a problem on it
- 6- a-The life cycle of Virus & Worms
b-the propagation of worms
- 7- a-Write the block cipher modes (EBC, CTR, C,,)
b- Draw the diagram for OFB
- 8- a- SSL session & SSL connection
b- 3 ways to do MAC
c- SET diagram and scenario steps
- 9- a- 6 requirements of public key
b- Attacks that ccan be handled with MAC
- 10- a- Why Stream Cipher is not recommended to use same key?
b- Requirements of strong hash fn.
c- compare between weak collision and strong collision?
- 11- a- What is SALT in UNIX password managment?
b- 2 different ways to keep a password file secure(I guess)?
c- 4 methods to get passwords that are not gessable
- 12- a large table related to SSL taking about each attach and how to overcome it ,
(copy paste from book)
- 13- A problem on firewall ,it looks similar to the table in the book
(src ,dst ,port , allow or disallow)