Frequency	Chapter	Question		
9	11	Hash Function requirements		
8	12	What types of attacks prevented by Message Authentication?		
6	21	Phases of the Virus & describe each		
6	3	Draw DES Round, describe it		
6	14	Draw Public-key authority diagram		
6	12	objective of HMAC		
5	14	State the requirements needed in any certificate issued by a certificate authority		
5	12	draw HMAC		
5	10	Diffe Helman algorithm		
5	20	What is honeypot? Used for?		
4	14	Draw Certificate Authority Diagram		
4	14	Describe Needham-Schroeder Protocol for distribution a shared key between two parties	Shared key using KDC	
4	20	3 classes of intruders		
4	6	5 modes + diagram of OFB + OFB adv & disadv	Mention modes of operation of DES.	
3	16	Draw SSL Protocol Stack		
3	16	Write Operations of SSL record protocol		
3	9	RSA algorithm		
3	20	Difference between statistical anomaly detection and rule-based intrusion detection	same as mention & describe two techniques for detecting intruders	
3	21	How does a worm propagate?		
3	20	Techniques to avoid guessable passwords		
3	2	What is the main drawback of the one-time pad?		
2	21	Types of Malicious Software		
2	6	Explain the Double DES and Triple DES and write the needed equations, draw diagrams		
2	11	What are the three ways to do authentication?		
1	12	Authentication Requirements		
1	16	Describe SSL services in one sentence		
1	16	What does SSL alert protocol do?		
1	16	SSL security records & its security services		
1	16	What is the difference between SSL session and SSL connection?		
1	20	What are two\four common techniques used to protect a password file?		
1	2	What is the one-time pad cryptosystem? What is it used for?		
1	14	Needham suffers from man-in-the-middle attack, explain.		
1	11	What is the difference between the weak collision resistance and the strong collision resistance?		
1	14	Needham suffers from man-in-the-middle attack, explain.		
1	14	Content of certificates	Timestamp - ID - Public key	
1	20	What is an Audit record? Why is it used?		
1	6	Why is it not good to encrypt two plain texts using the same key in stream ciphers?		
		Elgammal encryption, digital signature	علشان لا يلدغ مؤمن من جحر مرتين :D	
		فيه غير دول mcqs و مقارنات بين حاجات أو اسئلة بأرقام		