10 questions
3 bonus questions

Lec#	Ch#	Pg(s)	hint
6	5	14	what is a field? field properties (3-4)
		17	finite field of order p where p is a prime # (GF(P))
		18?	matricies for addition and multiplication
		32	$f(x) \times g(x)$ for a given field (w/ modulus) ($f(x) \times g(x) \bmod m(x)$)
12	6	22	what is avalanche effect + why is it important
			Discuss how confusion + Diffusion can be achieved in AES
		4	write the particular rounds in AES (1 sentence each)
13	7	?	How does 3DES work/draw diagram
		6	How does Meet-in-the-Middle attack work/draw diagram
		9	Modes of operations in AES
		17	2-3 scenarios (typical applications) which mode(s) apply from table
14	11	?	Difference between cryptographic hash function & Symmetric key enc.
		9	Explain how hash can ensure digital signature (diagram + 1-2 sentences)
		18	what is property to ensure collision resistance (talk abt variations)
15	9	10	draw diagram for how public key cryptography ensure confidentiality
		11	↓ Authentication
		12	↓ secrecy
		9	diff between conventional and public key encryption
		^	Given 2 prime # (ie. 13,7), find: mod(n), Totient $\phi(n)$, enc. exponent e, dec exponent d (rsa-updated.pdf)
16	10	4	Know how Diffie-Hellman works + draw diagram