

eman abdallah

SA

as long as i remember w isA yegyy

OSI arch page 7

anwa3 el attacks page 13

eman abdallah

SA

as long as i can remember:

chapter 1:

OSI arch. page 7

security attacks page 13

security services page 17

security mechanisms page 19

rasma zay page 21 :S :S kanet moseeba:S:S

chapter 2:

el vigenere attack page 45

One time pad page 48

Rotor machines(IMP) how does it work.. page 51

steganography .. zay el 7ebr el serry w el 7agat deeh .. el points elly f a7'er page

53w awel 54 goom ennena nektebhom w neshra7 w el drawbacks bayen w keda

dah ba2a elly fakrah bas i think geh meno keter..

chapter 3:

diffusion and confusion: page 67

ta2reban el points elly f a7'er 68 w 69 gaat (not sure)

el rasma page 74

el rasma page 77

el example 3ala el S blocks elly f page 78 geh zay ma hwa... bta3 el efgh..., defghi...

el avalanche effect page 80

entazerona ba3d el fasel 7ageb ba2y el chapters

salaam

Nesma K.

Assalamu alikum,
that's all what I remember...

for el mona2sat:

- anwa3 el ta2meen
- nesbet el ziada/noksan f 7agm el mona2sa
- the items included in el 3ard el fanny

for the security:

- Key distribution scenarios
- affine caesar cipher
- **ta2reban** compute the private key given the public key and an "easy-to-factor" n

eman abdallah

Chapter 4:

el rasma elly f page 100.. lel tafre2 been el group w el field wkan el matlob el far2 benhom bas el rasma deh is enough
modular arith.. page 101 geh bta3 el minus bayen(mesh sure)
gcd.. page 107, w el algo page 108 aw el algo el tanny page 111...aw el 2 bgad mesh fakra 7'ales bas wa7ed menhom aw el 2 gomm

chapter 5: magash meno 7aga :D,

ch 7:

compare link and end to end encryption page 205
page 209 feh 4 no2at keda ana fakra enny katabtohom fel exam
el session key page 214
random no generator page 218 ma3a eno kan mal3'y:S:S

ch9:

gat mas2ala f section 9.2 page 268
geh el RSA algo, el figure elly f page 270
ana kont katabt el algo elly f page 272 fel figure bas mesh fakra kan matlob wala et3'azt 3ashan kont fahmah f katabtoo
el toro2 to attack RSA, page 275 ettalabo nektebhom in brief

ch10

el 4 points bto3 page 291
geh rasmeten men 4... el rosomat zay bta3et page 293 bas ana mesh fakra anhy menhom geh, bas as i think bta3et el public key page 293, certificate page 294

w el kanoon kont ana ba3atow zaman.. bas hwa zad 3aleh mas2ala bta3et el sherka
elly et3arad 3aleha mona2sa b felos 10 000 bayen
then hya reg3et f kalamha

w el so2al el tanny bta3et el sherka elly me2adema el 3orod hya elly reg3et f
kalamha bas mesh fakrahom

hope that helps
rabena ma3ako
salam