Mid2010

1) Single round DES figure

82

single round of DES attack figure (page 77)

2) DES key exchange figure
http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.csfb500/csfb5za021.htm

3) Multiplicative inverse using extended Euc. alg.

112 ch4

4) RSA p,q key pair generation and encryption/decryption technique

CH9 page 15

5) Group, Ring , Field

116

(2-5two binary numbers multiply them in GF(2^3) , m(x)= X^3 +X +1

GF(in notation xiii

6) mod(29), GF(2^6), GF(2^8), mod(16) which of them can be used to encode binary data,which can be used but will increase the number of bits, which can't be used and why?

7) Traffic Padding : def, why using it?
23

8) Arabic rotor machine 29 characters , 4 rotors... how many different substitutions?why?
55

9) if 6 rotors ,,how many diff. subs and why?

55

Notes(2)

ch2:

p .40 Playfair cipher

p.51 Rotor machine

p.53 Steganography (Definition only)

ch3:

p.72 data encryption standard

Draw the diagram p.77 and discuss their functionalities

ch7:

p.203 Compare between link encryption and end to end encryption

p.213 state the key distribution scenario

ch.1,4,6 are included also in the exam but i don't know what is the most important sections in them

Exam question 2007

Chapter 1

- Compare active attack to passive attack, giving an example for each

Chapter 2

- Using this Playfair matrix

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

- encrypt this message:
- Must see you over Cadogan West. Coming at once.

Chapter 3

- What is meant by a timing attack? Compare with brute force attack.

Chapter 4

- Multiply 01010111 by 10000011 in GF(2^8) modulo $m(x)=x^8+x^4+x^3+x+1$

Chapter 7

Compare Link Encryption to End-to-End Encryption, and which do you think is more secure and why?

Security 2007 Final

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

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

Chapter 4:

el rasma elly f page 100.. lel tafre2 been el group w el field w ....kan 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

2008

حاجات اتعملت بالاصفر فوق

4.6 For each of the following equations, find an integer that satisfies the equation.

a. b. c.

9*x* K 8 (mod 7) 7*x* K 6 (mod 5) 5*x* K 4 (mod 3)

X

there was also a question about the Avalanch effect

the answer by the way is that

A small change in either the plaintext or the key should produce a significant change in the ciphertext

Muhammad El-Nabawy ch 1 slide 10