Questions

1

(a) Page 34, chapter 2

- Unconditionally secure: if the ciphertext generated by scheme does not contain enough information to determine uniquely the corresponding plain text, no matter how much time or ~~chi~~ ciphertext is available.
- Computationaly secure:

  if the cost of breaking the cipher exceeds the value of encrypted information.

  OR if the time required to break the cipher exceeds the useful lifetime of the information.

1

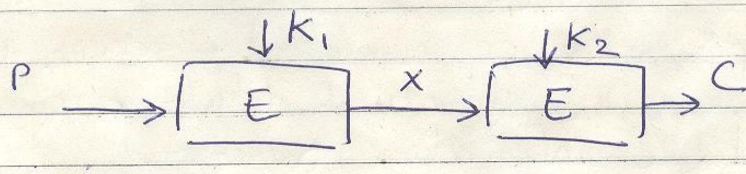
b) page 176, chapte 6

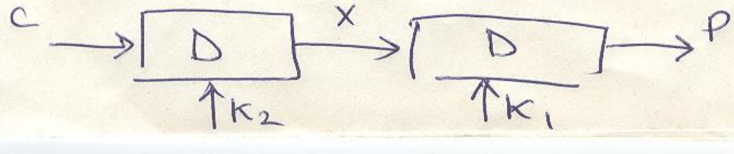
given plaintext p and two encryption keys K_1, and K_2 we obtain C as

$$C = E(K_2, E(K_1, P))$$

For decryption

$$P = D(K_1, D(K_2, C))$$





Question (4)

c) page 177, chapter 6

Due to meet-in-the-middle attack,

$$\therefore C = E(K_2, E(K_1, P))$$

$$\therefore X = E(K_1, P) = D(K_2, P)$$

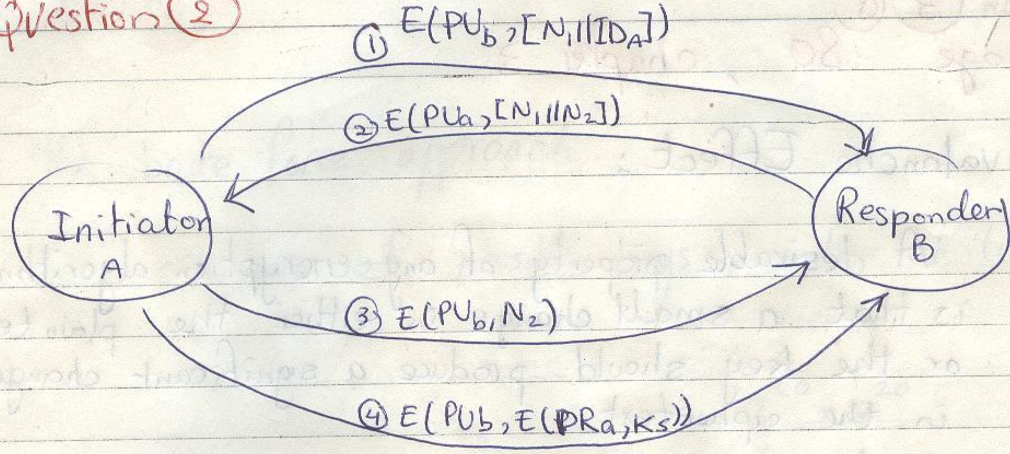
so, given a known pair (P, C)

the attack

1. Encrypt P with all 2^{56} possible values. and sort the result according to
2. decrypt C with all 2^{56} keys

if a match occurs

Question (2)



chapter 10.

Page 291, 296, 297

Question (3)(a)
page 80, chapter 3

Avalanche Effect:

A desirable property of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text.

Question (3)(b)
chapter 1, Page 12

the OSI architecture focus on.

(1) Security attack:
Any action that compromises the security information owened by an org

(2) Security mechanism:
A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security mechanism.

(3) Security service:
A processing or communication service that enhances the security of data processing systems and the information transfer.

Question 4

* the brute force approach.

number of possible keys = number of trails

$= 2^{40}$

$= 2^{20} * 2^{20}$.

∵ each 2^{20} trail can be done in 1 sec.

∴ required time = 2^{20} seconds.

* practicle if the data is still useful after spending 2^{20} sec.

* Not practicle if approach when the key is changine every less than 2^{20} sec.

Question 5

if we know $\underbrace{e, n}_{\text{Public key}}$ and $\underbrace{d, n}_{\text{Private key}}$

since
for encryption

$$C = M^{e} \bmod n$$

and for decryption

$$M = C^{d} \bmod n$$

the question can be if we know e, d, and n can we get $\Phi(n)$

since

$$d_1 \equiv e_1^{-1} (\bmod \Phi(n))$$

and

$$d \equiv e^{-1} (\bmod \Phi(n))$$

~~whe~~ Where

$$d_1 e_1 \bmod \Phi(n) = 1 \quad \rightarrow (1)$$

and

$$d e \bmod \Phi(n) = 1 \quad \rightarrow (2)$$

From equation (2) we can ~~que~~ list the possible values of $\Phi(n)$ given d, e

then check these ~~..~~ values on equation (1) to get d_1

Question 6   Chapter 4, Page 97, 98

A group: $\{G, \cdot\}$ a set of elements with a binary operation with the following axioms are obeyed.

1. Closure $a.b$ also in G
2. Associative $a.(b.c) = (a.b).c$
3. Identity element $a.e = e.a = a$
4. Inverse element $a'.a = a.a' = e$.

A ring: $\{R, +, \times\}$ a set of elements with two binary operations, called adition and multiplication, such that the following axioms are obeyed.

$\underbrace{\text{(1) Closure, (2) Associative, (3) Identity element (4) Inverse element (5) Commutative}}$

↓ is an abelian group with respect to addition.

+ (6) Closure under multiplication

(7) Associativity " "

(8) Distributive laws

Question 6

A field: set of elements ~~aba~~ obeying the following

is an integral domain.

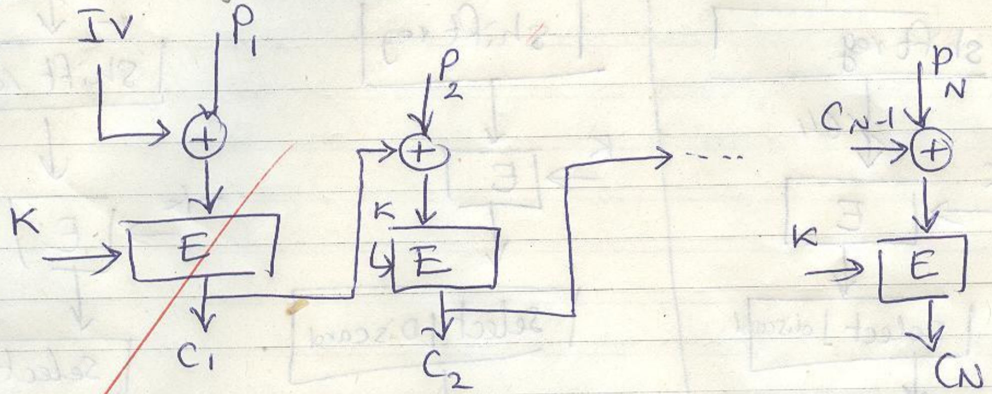
1 – 8

+ 9 Commutative under multiplication
10 Multiplicative identity
11 No zero divisors.

12 Multiplicative inverse.

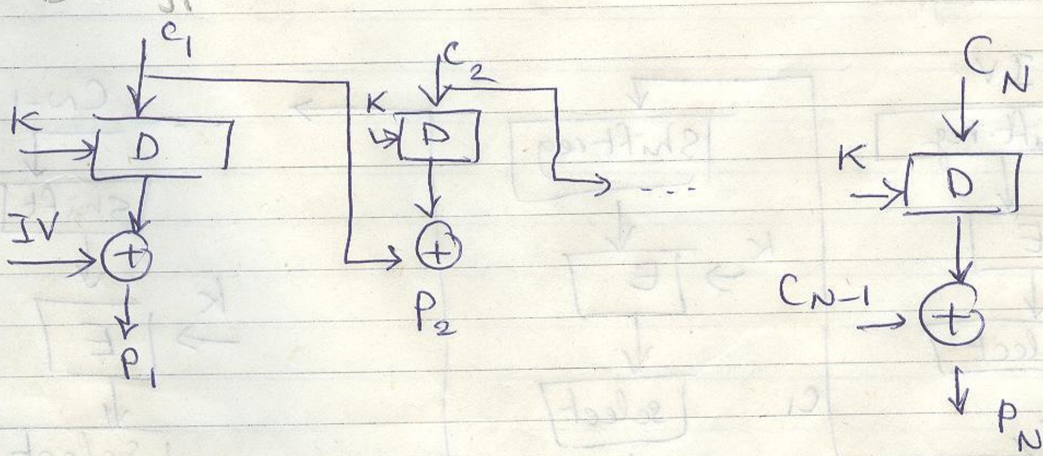
Question (7) page 183 chapter 6

a) Encryption



$$C_i = E(K, [C_{i-1} \oplus P_i])$$

Decryption



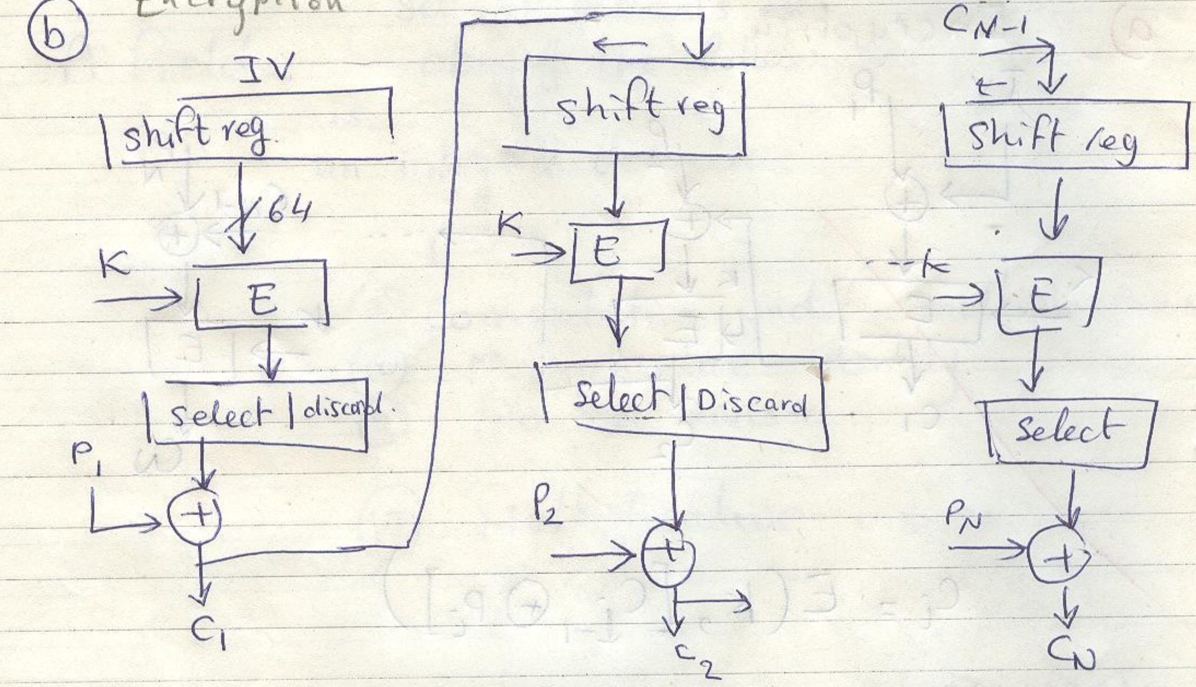
$D\{/=$

$$P_i = C_{i-1} \oplus D(K, C_i)$$

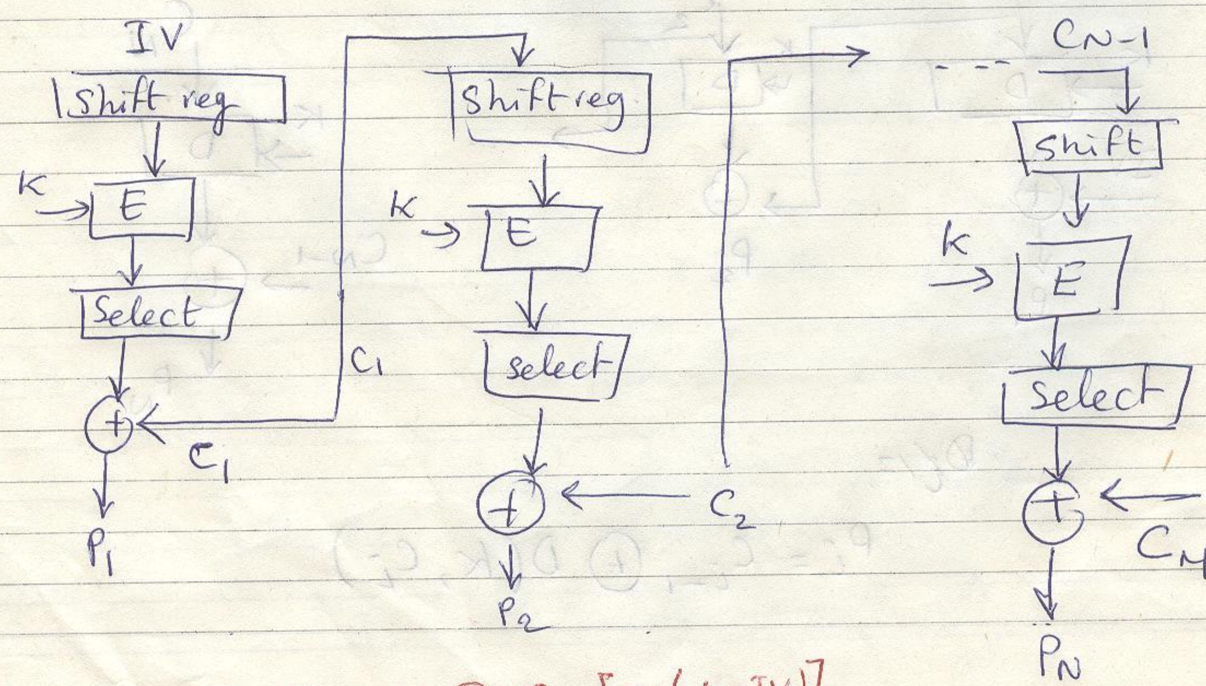
Page 185 chapter 6

Question 7 $\qquad C_1 = P_1 \oplus S_s[E(K, IV)]$

b Encryption



Decryption



$P_1 = C_1 \oplus S_s[E(K, IV)]$

~~Shift~~ select shift