NETWORK SECURITY

* Stallings

footnote:

A for projects

Cryptography in 'C'

Bruce Schneier

* GATE SYLLABUS

- ✓ principles of private & public key cryptography
- ✓ Digital signature
- ✓ firewalls

* Security Components

1. Confidentiality
2. Key Management
3. Authentication
4. Digital signature
5. Compression

* Email Security PGP - pretty good privacy Pem

Privacy enhanced mail.

1	✓	✓
2	✓	✓
3	✓	✓
4	✓	✓
5	✓	✓

Confidentially

cryptology

cryptanalysis

cryptanalysis & breaking

Terminology

P = plaintext → data format

C = Cryptic text → ciphertext

E = Encipterment

D = Decryption

So E and D are mutually

each other.

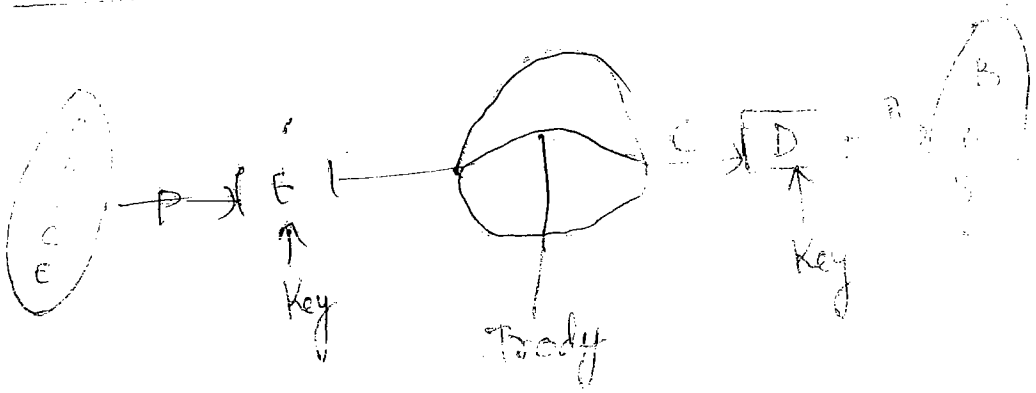
principle = comm parties → Alice, Bob

Intruder = unauthorized person → Trudy

Passive

Active

TRADITIONAL MODEL FOR CRYPTOGRAPHY



CLASSICAL ENCRYPTION ALGORITHM

I K- shift Method or Ceasar Method

Ex: ① K = 3

P = BAL

⇒ C = EDQ

② C = L D P D E R B

P = ~~I B N D B E X~~

P = I A M A B O Y

Approach of Cryptanalyst

Monograms = { I, a

Digrams = { am, an, at, as

{ I - - -

Monograms will give clue to digra
Digrams will give clue to Trigra
and so on

Here C = L D P D E R B

k c o c d z q

P = I a m a B o y

II Substitution Algorithms

a) Monoalphabetic Substitution Algorithm

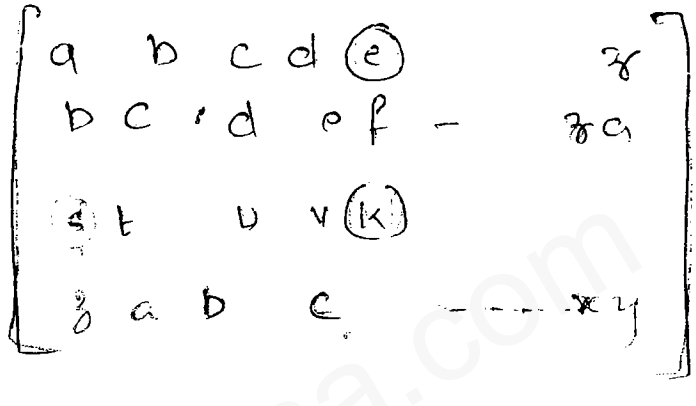
Ex Mapping Table

a	s
b	u
c	r
d	a
e	h

P = BAD

C = USA

(GOALS)



(ii) TRANSPOSITIONAL METHOD

Plaintext: WE ARE DISCUSSING NWS ~~AT~~ IN ROOM NO #404

Key = M E G A B U C K
= 7 4 5 1 2 3 6

(By numbering as in alphabetical order)

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
W	E	A	R	F	D		C
S	C	U	S	S	I	N	G
N	K	S	I	N	R	O	O
M	N	O	#	4	O	4	

Key size / No: of char. received / No: of full rows

C = RSI#ESN4INC4ECWNAL SGC KISNMDIRO

No. of chars received = 31

$$8 \overline{)31}\ 3,\ 24,\ 7$$

So there is 3 full rows and other row of 7 letters

KEY

SYMMETRIC (or) Private Key Cryptography

ASYMMETRIC Public Key Cryptogra

Ks shared key
Session Key

(Ex) ✓ DES (56 bit)

- triple

✓ IDEA (128)

present AES (128, 192 ...)
(adv. encryp. std)

adv : fast

Disadv : Key Distribution

(Ex) : i) RSA & MH
ii) Rivest
iii) Knapsack

appl? ✓

✓ Authentication

Disadv

the session key between the sender a

$x^y \bmod n = 3^{10 \times 8} \bmod 47$

$= 3^{80} \bmod 47$

$= 4$

4. The total number of keys required for a set of individuals to be able to communicate with each other using secret key and public key cryptosystem respectively are.

If 4 individuals

private key crypto

	1	2	3	4
1	x	✓	✓	✓
2	x	x	✓	✓
3	x	x	x	✓
4	x	x	x	x

Here, 6 key required

ie, $\frac{n(n-1)}{2}$

for public key cryptosystem

(Ans) $n(n-1)/2$ and $2n$

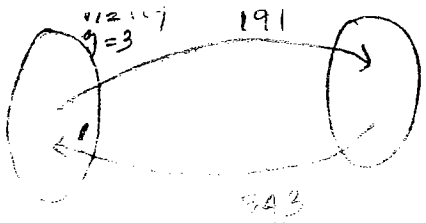
Diffie Hellman key exchange algo. is used The sender sends (719, 3, 191) and the receiver responds with 543. If the receiver's secret key is 15 then calculate the shared key.

$n = 719$

$g = 3$

$3^x \bmod 719 = 191$

$3^{15} \bmod 719 = 543$



Session key = $(191)^{15} \bmod 1147$

= 40

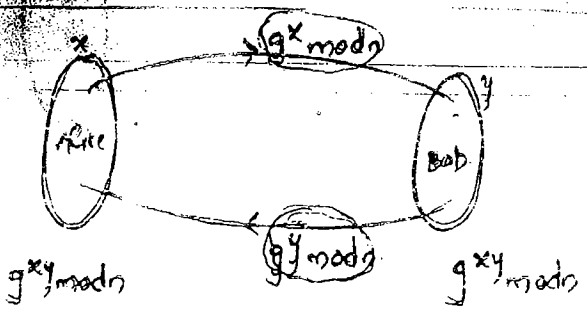
12/11/10
FRIDAY

DATA ENCRYPTION STANDARD (DES)

- ✓ Devised @ IBM
- ✓ Based on monoalphabetic [illegible]
- ✓ Attack = Leslie
- ✓ proof = feistel
- ✓ Input = 64 bit = block (plaintext)
- ✓ Output = 64 bit = ciphertext
- ✓ Key = 56 bit
- ✓ Total = (19) stages.
- ✓ In that (16) stages are key dependent and iterative in nature
- ✓ stages are key independent {16+3 = 19}

KEY MANAGEMENT

DIFFIE HELLMAN KEY EXCHANGE ALGORITHM (DH Al



x - Secret key sender

y = Secret key of Rece

$g^{xy} \bmod n$ - Session

Good Candidate

Choose 'N' in such a way that N and $\left(\frac{N-1}{2}\right)$ bot prime numbers

Eg: N = 7

$$\frac{(N-1)}{2} = \frac{(7-1)}{2} = 3$$

② N = 47

$$\frac{(N-1)}{2} = 46/2 = 23$$

FAST EXPONENTIAL MODULAR ARITHEMETIC

$M^e \bmod n$

e = expand in binary

Initially d = 1

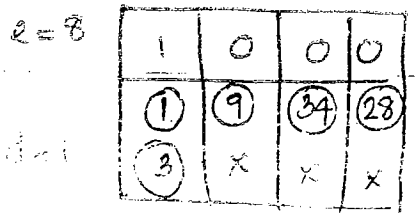
Until e^t bits exhausted

$d = (d \times d) \bmod n$

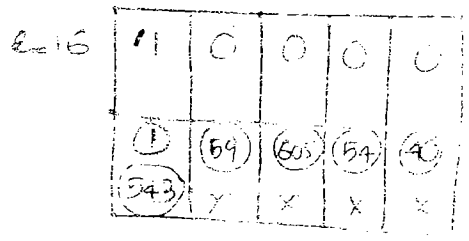
If $(b_i = 1)$

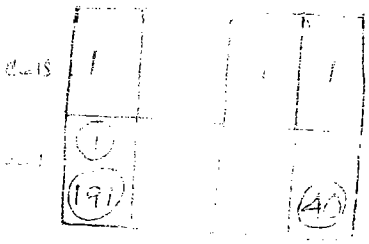
$d = (d \times M) \bmod n$

Eg: ① $8^8 \bmod 47$

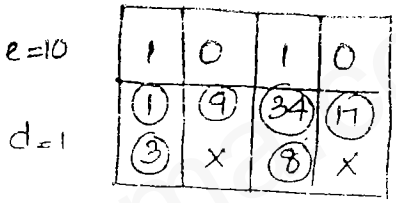


② $543^{16} \bmod 714$

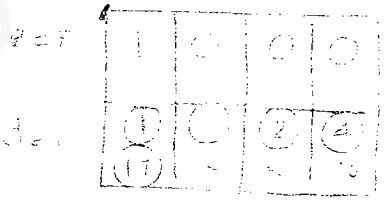




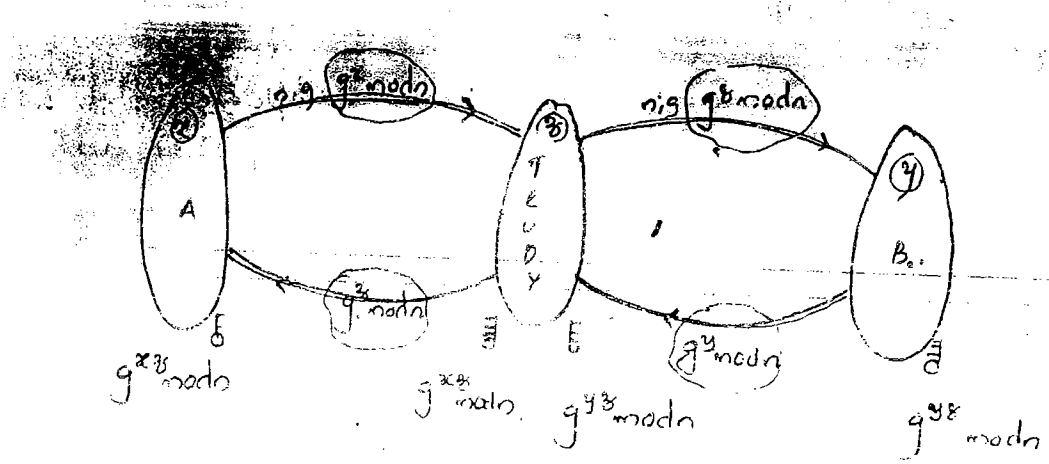
③ $3^{10} \bmod 47$



④ $17^8 \bmod 47$



ATTACK ON DH ALGORITHM



Man in the middle Attack (or)

Bucket Brigade Attack.

Problems

1. Which of the following is a good candidate for N for Diffie-Hellman protocol?

A) 7 B) 33 C) 37 D) 47

A) $N = 7$

$\frac{(N-1)}{2} = 6/2 = 3$ (prime) ✓

B) $N = 33$

$\frac{(N-1)}{2} = \frac{32}{2} = 16$ (not prime) ✗

C) $N = 37$

$\frac{(N-1)}{2} = \frac{36}{2} = 18$ ✗

D) $N = 47$

$\frac{(N-1)}{2} = \frac{46}{2} = 23$ ✓

2. The Diffie Hellman Key exchange is being used to establish a session key between the sender and the receiver with the values of $g = 7$, $n = 23$

a) If the sender's secret key is $x = 3$ Then it transmits the msg (23, 7 ___)

$g^x \bmod n = 7^3 \bmod 23$

$= 21$

b) Receiver's secret key $y = 15$ and if it responds with the message (____) fill the blank.

$g^y \bmod n = 5^3 \bmod 23$

$= 7^5 \bmod 23$

$= 11$

c) What is the session key between the sender and the receiver?

$g^{xy} \bmod n = 7^{5\times 3} \bmod 23$

$7^{15} \bmod 23$

1	1	1	1
1	3	4	2
7	21	5	14

Ans = 14

3 The Diffie Hellman key exchange is being used to establish a session key between the sender and the receiver with the values of $n = 47$, $g = 3$

(a) If the sender's secret key is $x = 8$ then it transmits the msg (47, 3, ____) fill in the blank

$3^8 \bmod 47$

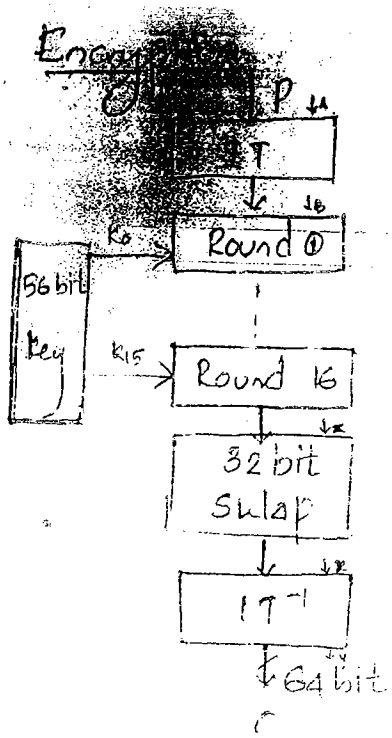
$= 28$

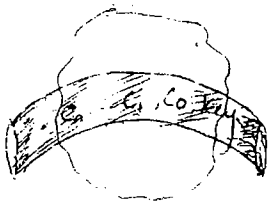
1	0	0	0
1	9	34	8
3	x	x	x

(b) Receiver's secret key $y = 10$ and if it responds, with the msg (____) fill the blank

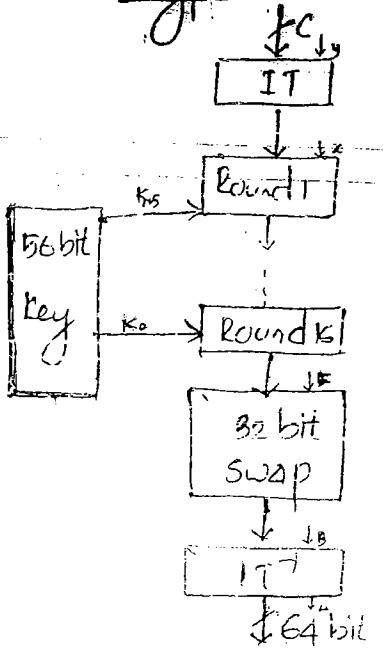
$g^y \bmod n = 3^{10} \bmod 47$

$= 17$





Decryption



(8)

IT

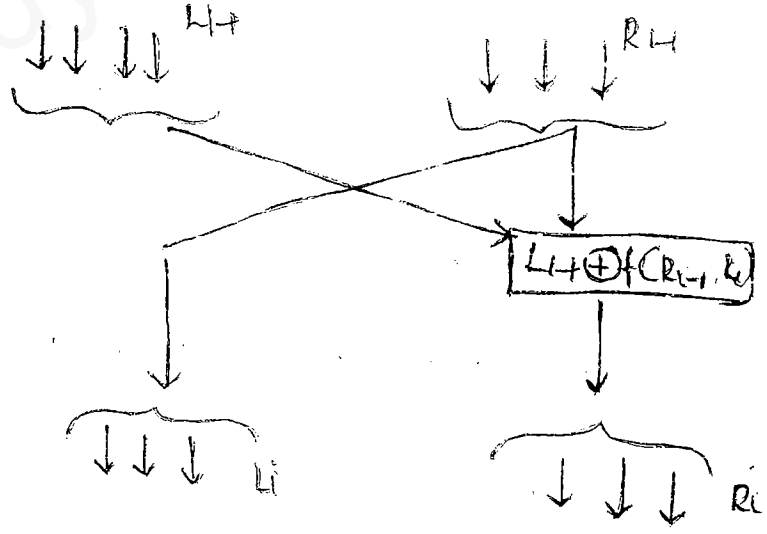
0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6

IT⁻¹

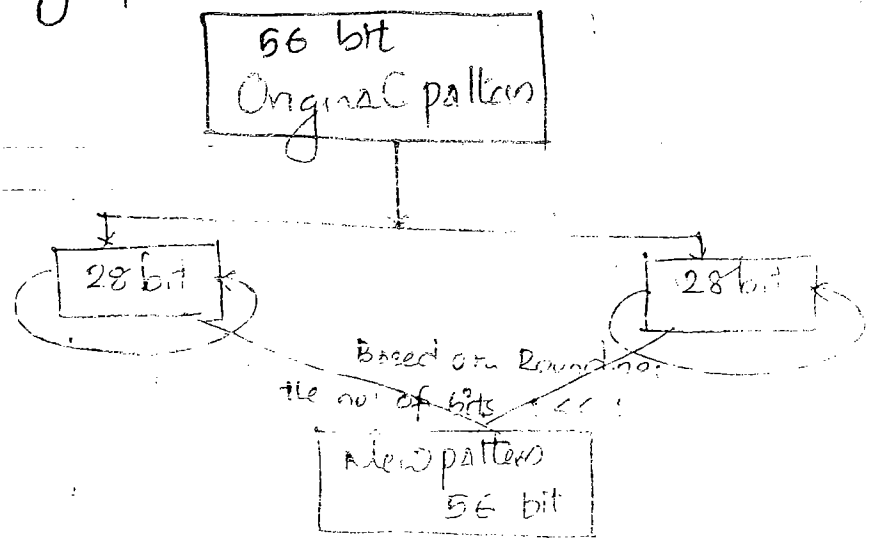
0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6

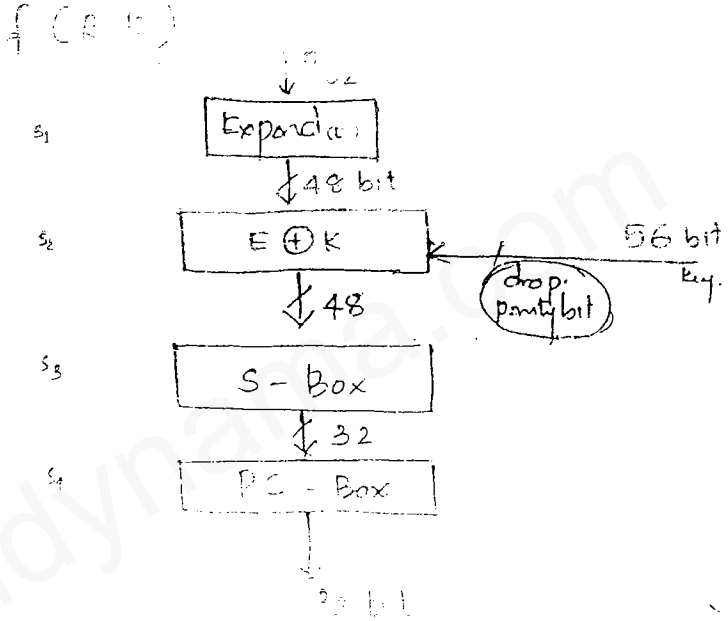
It is a symmetry

Round



Subkey Generation



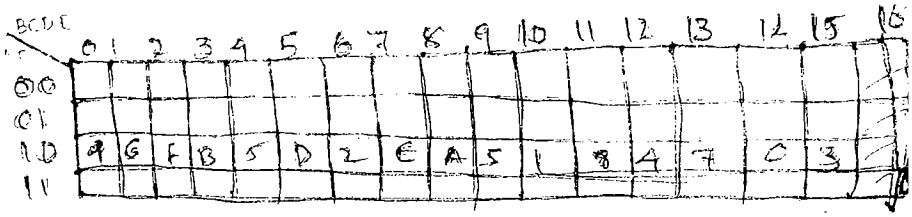


If no of 1's is odd t
If no of 1's is even t

Expand

8 × 4 = 32 → 8 × 6 = 48

S-Box

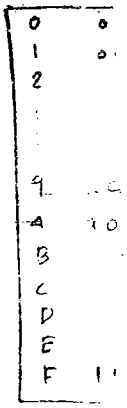


If input is S box is

goto AF and take 10 in

put is 0000

1 1 0 0 0 0



Here AF = 10 BCDE = 1000 & 8

So output of S-box is 'A' = 1010

Fiestel proof

$IT(A) = B$

$A = IT^{-1}(B)$

$IT^{-1}(x) = y$

$x = IT(y)$

Keying Encryption & K_0 to K_{15}

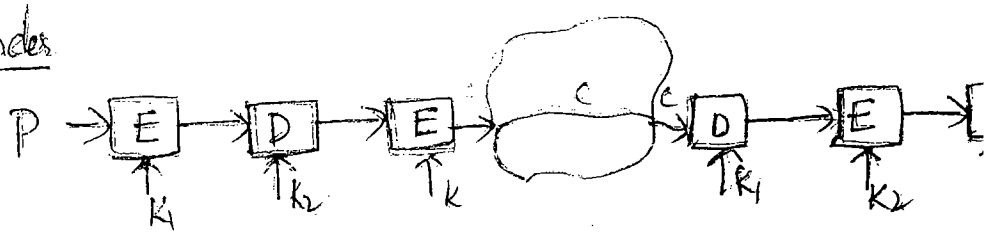
Decryption & K_{15} to K_0

Note

* $D(E(P)) = P$
* $E(D(P)) = P$

TRIPLE DES

* Encryption with 3 keys
* But DES is come with 128 bit key only
* So now-a days Triple DES with 2 keys



$D_{K_1}\ E_{K_2}\ D_{K_1}$ (C)

→ $D_{K_1}(E_{K_2}(D_{K_1}(E_{K_1}(D_{K_2}(E_{K_1}(P))))))$

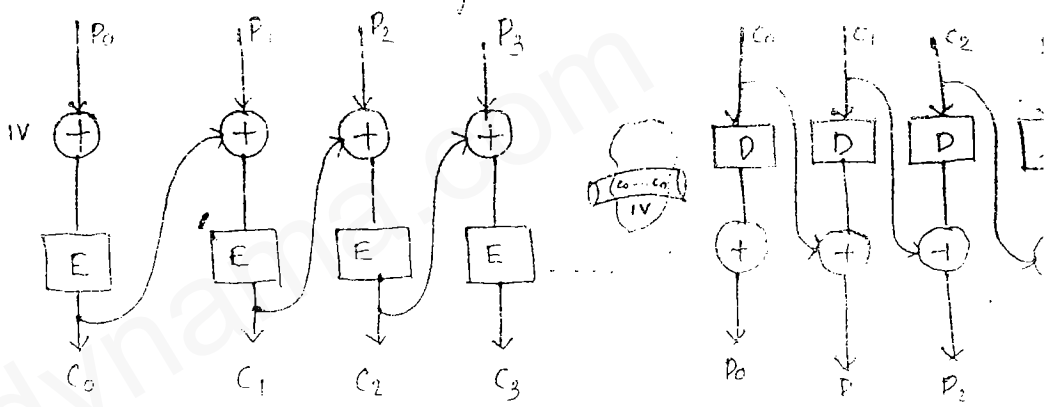
Modes

1) Electronic Code Book Mode

Leslie Attack - Cipher Block chaining

* Manipulation is done on ciphertext and got financially benefited

Goal: Even though the plaintext when ciphertext are repeated the ciphertext should not be repeated



Encryption

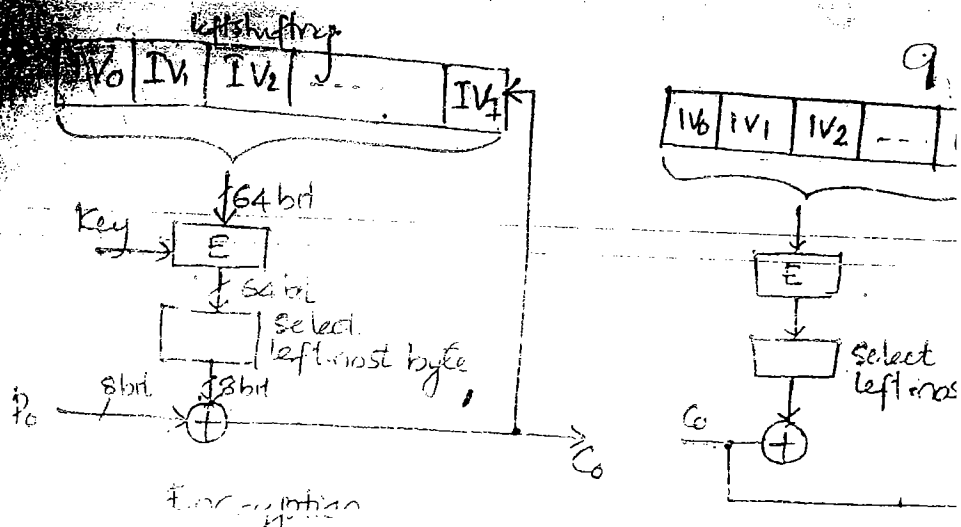
Decryption

* Error causes impact on two blocks only [illegible] and [illegible]

* Bit timing error causes the impact [illegible]

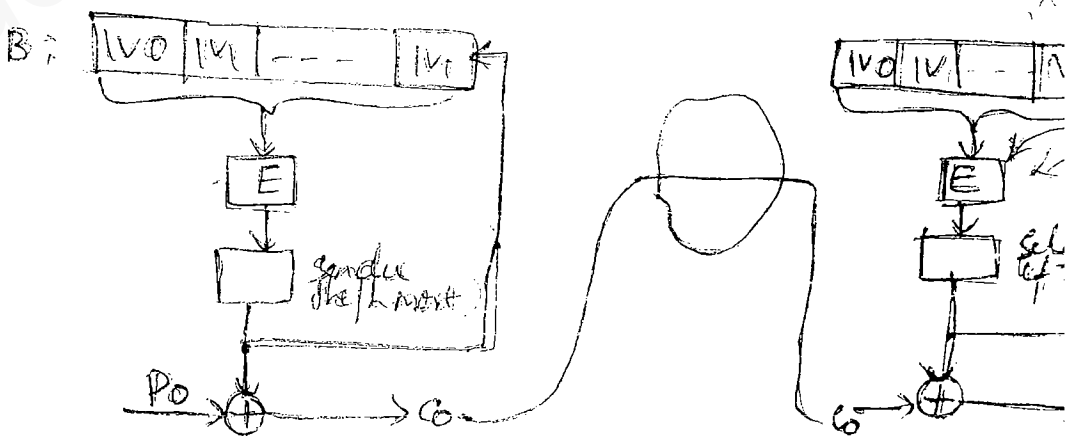
Cipher Block feedback mode

* Used when the input size is less than block size



* Only [E] box is sender and receiver left shift register (LSR) is used by both sender and receiver
* Both LSR should be synchronised
* Bit error causes its impact on two by Only (ie. i^{th} and $i+8^{th}$)
* Bit timing error causes its impact on all subsequent bytes
* feedback is required for not to have Leslie attack

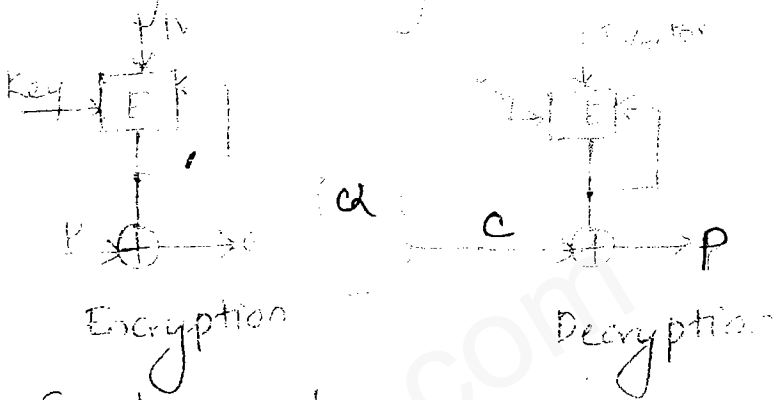
4. Output feedback mode



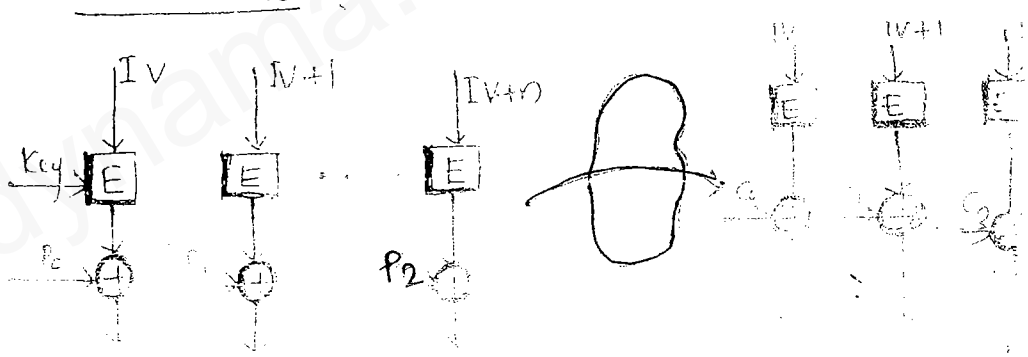
* Let ith byte error should not cause its impact on subsequent bytes, so the feedback is considered from the o/p end

This mode is not robust because cryptanalyst can easily break this. Since it works on the cyclic data.

5. Stream cipher



6. Counter Mode



→ Now a days the database

→ Not to depend on the preceding second C to decrypt the individual (second) counter is attacked. The counts will be all No SSN DAN Card No or any Unique identifies

Modes is practice real world

↓

input

[diagram in booklet]

Largesize → chaining is used (ii)

block size → feed back is used (iii)

(i) (ii) (iii)

13/10/10 SATURDAY

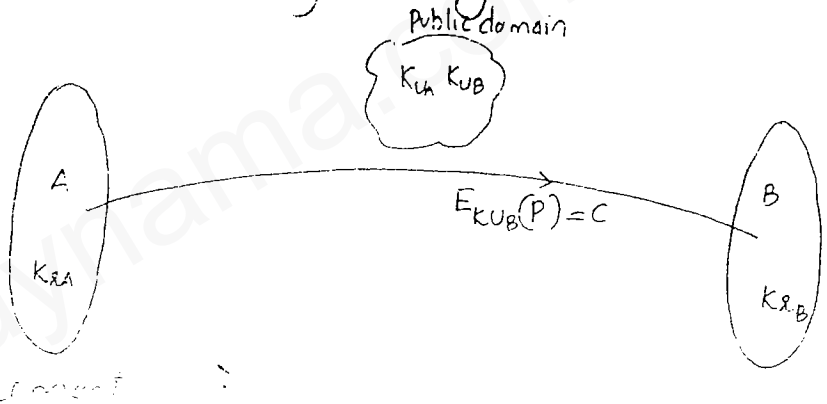
PUBLIC KEY CRYPTOGRAPHY

Assymetric Key Alg

Two keys

↳ One key = Encryption = public key (K_u)

Other key = Decryption = private key (K_R)



Advantage

* Eve ... type ... diff the above ... possible just because both keys are originated by the same ...

$D_{K_{R_A}}(E_{K_{U_A}}(P)) = P$

* One cannot guess (K_R {private key}) from K_u public key ($E_{as}\{K_u\}$)

$E_{KU_B}(\star) = C$

RSA ALGORITHM (Rivest, Shamir, Adleman)

1. Choose two large primes p & q
2. Compute $n = p \times q$ and $z = (p-1) \times (q-1)$
3. Choose a number, relatively prime to z and call it d
4. Find e such that $e \times d = 1 \bmod z$

$$ed \bmod z = 1$$

Encryption

$KU = \{e, n\}$

$p^e \bmod n = C$

Decryption

$KR = \{d, n\}$

$C^d \bmod n = p$

Eg: ① $p = 3$, $q = 11$

② $n = 3 \times 11 = 33$

③ $z = 2 \times 10 = 20$

④ $(e \times 7) \bmod 20 = 1$

$21 \bmod 20 = 1$

$e \times 7 \bmod 20 = 1$

$e = 21/7 = 3$

Say

Ans Both are true.

3 The minimum the integer p such that $3^p \bmod 17$

Soln

$3^5 \bmod 17 = 5$

$3^8 \bmod 17 = 16$

$3^{12} \bmod 17$ = Calculator out of bound

So $n = 3$ $e = 12$, $n = 17$

4. MD5 hash alg create a 128 bit msg digest out of a msg of 512 bit blocks. It has message digest of 128 bit

5 Diffie Hellman key exchange is being used to establish a session key btw the sender & the receiver with the values of $n = 23$, $g = 7$

(a) If the sender's secret key is $x = 3$ then it transmit the msg (23, 7, ___)' fill in the blank.

$7^3 \bmod 23 = 21$

(b) Receivers secret key $y = 6$ he responds with the msg ___

$7^6 \bmod 23 = 1$

(c) What is the session key btw sender & the receiver

$g^{xy} \bmod 23 = 7^{6 \times 3} \bmod 23$

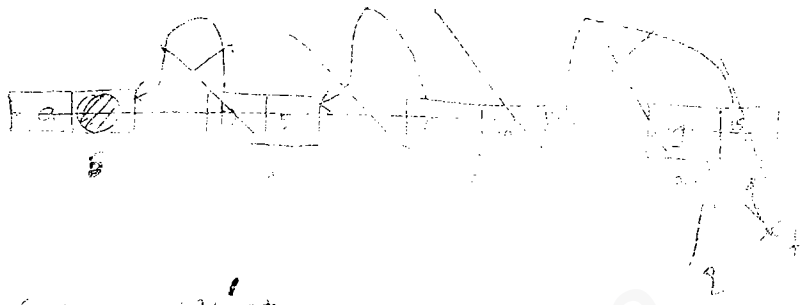
$= 18$

M = 7, e x 18, n = 23

e = 18	1	0	0	1	0
d = 1	1	3	9	12	18
	7	x	x	15	x

a SLC

QUESTIONS



1 Suppose that two parties A & B wish to exch
a common secret key btw themselves using
diffie Hellman key exchange tech. They agree on
as the modulus and 3 as the primitive root
party A choose 2 and party B chooses 5 as
their respective secrets their D-H key is

$$g^{xy} \bmod n$$

2 Consider the following statement
(i)
Perform a permutation of the elements
of its input alphabet

Ans bijective function means only one functi
have only one mapping No NA function co
map to one.

6. The RSA Alg. is used by choosing two prime no's say p=7 & q=17 If the public key is e=5 then

(1) What is the value of d?

(2) What is the cipher value to transmit the character F

(3)

x_1	x_2	x_3	y_1	y_2	y_3
1	0	96	0	1	5
0	1	77	1	-19	1

$\Phi = \lfloor x_3/y_3 \rfloor$

$q = 11$

$96 + 19 = 77$

(2)

$p = 6$

$p^e \bmod n = 6^5 \bmod (7 \times 17) = 41$

7. RSA alg is used with prime no: 397 & 401 to generate public keys & private keys.

(1) If the e is chosen as 343 then calculate 'd' value

$(343d)$

$(343\ d)$

		x_3	y_1	y_2	y_3	
1	0	159201	0	1	343	461
0	1	343	1	-461	277	1
1	-461	277	-1	462	66	4
1	462	66	5	-2309	13	5
			-26	12007	1	

$d = 12007$

(8) Diffie Hellman key exchange alg is used ... sends $(7, 3, 7^3 \bmod 23)$ and the receiver responds with $(76 \bmod 23)$ then calculate the session key

$7^{18} \bmod 23$

$((7^9 \bmod 23)(7^9 \bmod 23)) \bmod 23$

Ans $= 18$

(a) $a = 18$

$d = 1$

i	0	0	1	2
	1	3	9	12	18
	7	x	x	15	x

(9) sha1 hash algorithm create an N bit message digest out of a msg of 512 bit blocks. It has a msg digest of

5 words of 32 bits. $5 \times 32 = 160$

(10) Which of the following statements are true pertaining to the characteristics of digital signature

i) The receiver can verify the claimed identity of the sender

ii) The receiver can verify that the contents of the message have not been altered

iii) The receiver cannot possibly have composed the msg himself

Ans I, II & III

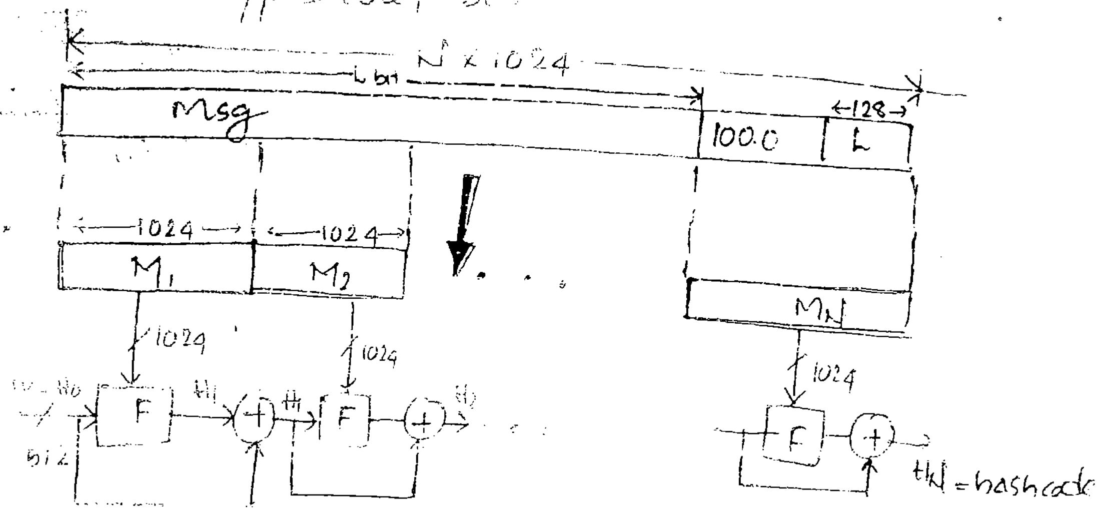
(11) Diffie Hellman key exchange ... the sender sends (7, 3, 19) and the receiver responds with 543 if the receivers secret key is 19 then calculate the session key

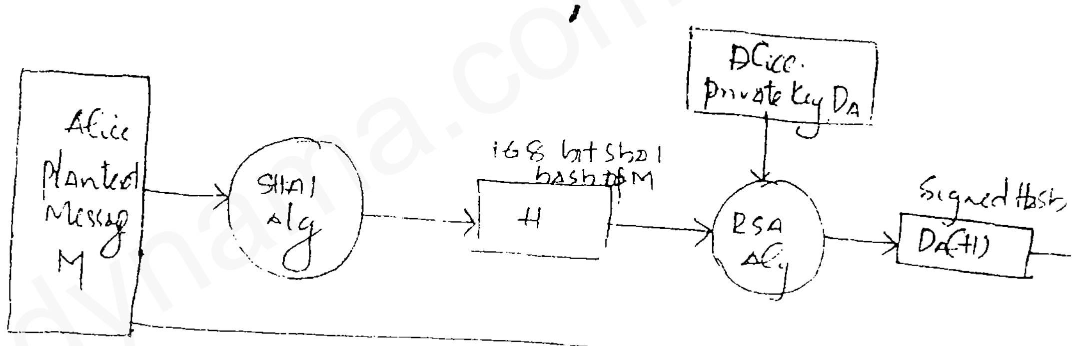
Observation

sha-512

o/p = 512 bits

i/p = 1024 bits

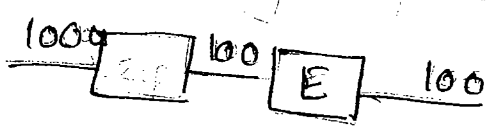




Observation

(1) we Do encryption first then zip

(2) we are doing zip then encryption

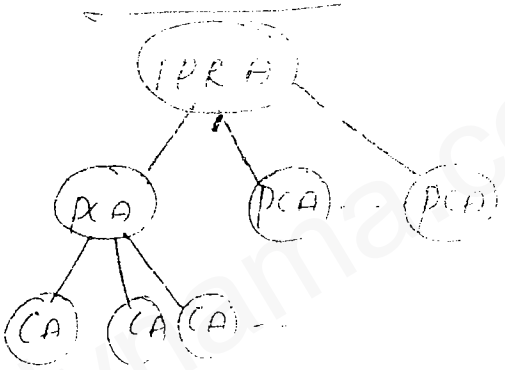


Second is fast because only 100 bits are need to encrypt

Email Security

~~Devised by~~	PGP (Pretty Good privacy)
Devised by	, plus ~~PEM~~
Confidentiality	IDEA
Key mgmt	RSA ; Diffie-Hellman
Auth ; Digital Sig.	RSA + MD5
Compression	

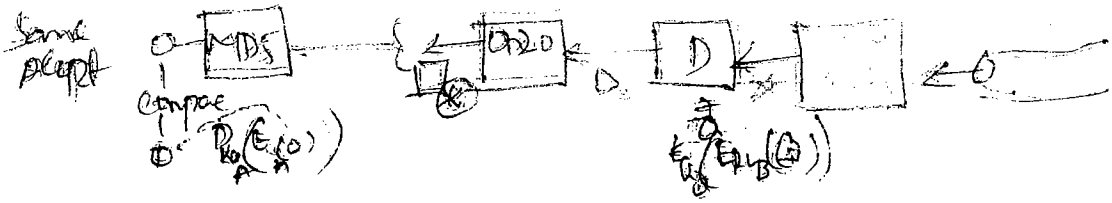
IPRA (Internet Policy Registration Authority



PCA - Policy Certification Authority

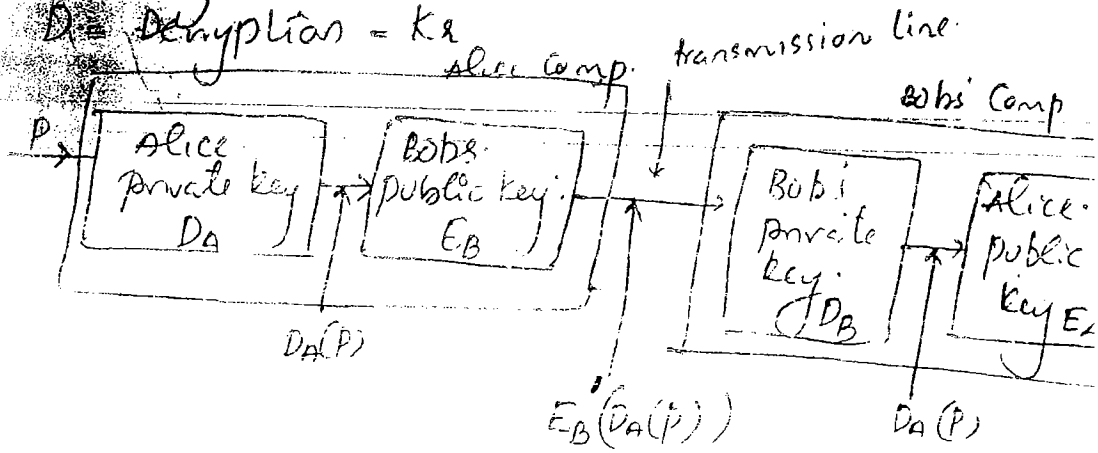
CA - Certificate Authority

Keyring = Ku + Ku + additional



E = Encryption = K_U

D = Decryption = K_R



Message Digests Alg ~~(MD5)~~

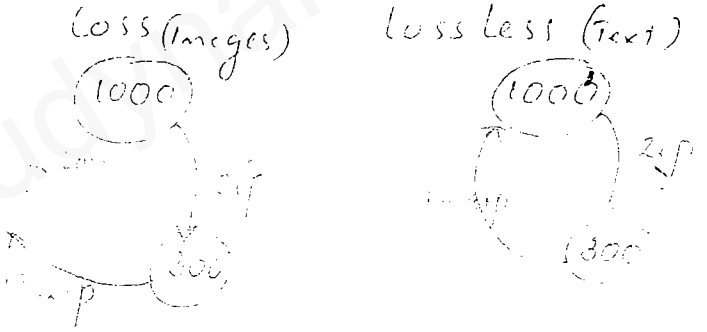
~~MD5~~

Digest

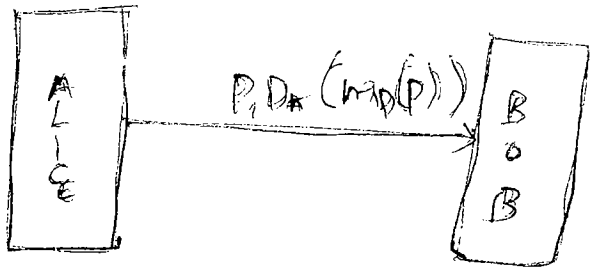
→ One way

→ The other way is ~~dige~~ impossible (One directional)

Compression → Bidirectional



MD5



MD5

- Message digest version 5
- o/p = 128 bits
- I/p = 512 bit
- ABCD = 4 registers
- each = 32 bit
- 4 × 32 = 128

SHA1

- Secure hash algorithm
- o/p = 160 bit
- I/p = 512 bit
- A, B, C, D, E registers
- each = 32 bit
- 5 × 32 = 160

- Given p' it is easy to compute MD(p')
- Given MD(p) it is effectively impossible to find p'
- Given p none can find p' such that MD(p') = MD(p)
- A change to the length of even 1 bit produce a very diff o/p

procedure for message digest

1. Append pad bits
2. " Length bit
3. Initialize buffer (IV)
4. process the message

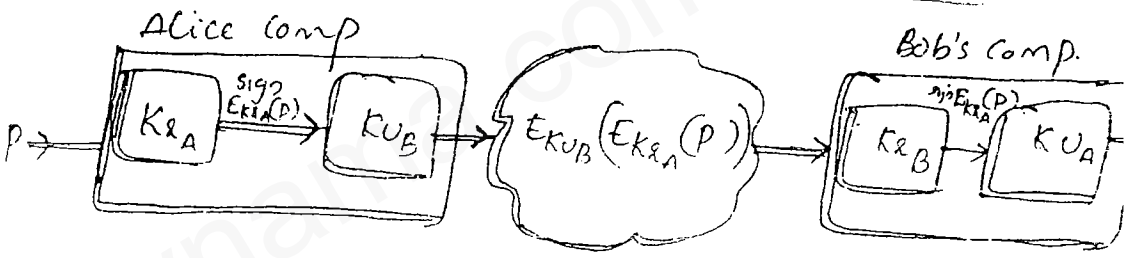
padding bit are append only to make the bit length a multiple of 512

Transmission overhead – If msg is imp for every encrypted msg, the big signature has to be sent so transmission overhead

2009 Gate Q. **Confidentiality** : A sender is employing PKC for sending a secret msg to receiver. Sender issues receivers public key

2007 Gate Q. **Digital signature**: A sender is employing PKC for sending a signed msg to the receiver. Sender uses his/her own private key

DIGITAL SIGNATURES USING PUBLIC KEY CRYP.



Adv

* No big brother
* No transmission overhead

With private key of A, message is encrypted with public key of B

Disadv

* memory overhead is there – we have to store the

Signature

DIGITAL SIGNATURE

Requirements

* The Receiver can verify the claimed identity of the sender
* The sender cannot later repudiate the contents of the message
* The receiver cannot possibly have composed the message himself

Protocol

Digital signatures with Big Brother

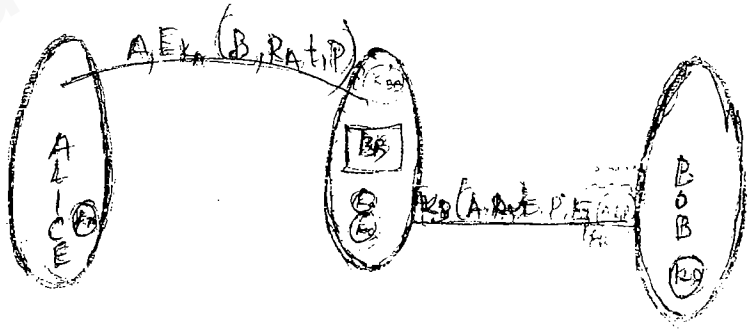
BB = Bigbrother = trusted / common friend of Alice & Bob

K_{BB} = Secret key with (BB) used for signature

K_A = Shared key b/w (A) and (BB)

K_S = Shared key b/w (BB) and (B)

t = time stamp
R = Nonce
} Not to have replay attack



Robin with $E_{K_{BB}}(A, t, P)$

Disadv
1 What if BB ?!!!
2 Transmission overhead } Sign is Big
3 Memory overhead

First two handshakes: using [illegible]

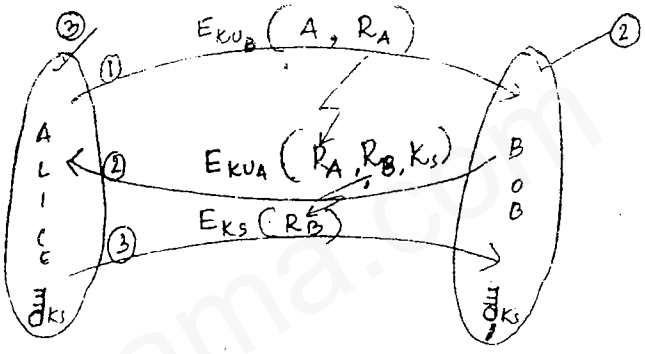
The third handshakes: using Symmetric (same Ke

R = Random No: = UNIQUE identifier
= Nonce
= Challenge / Respons

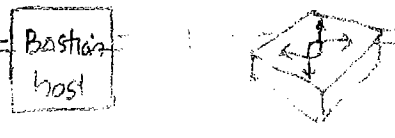
Ks = shared key / session key.

Multiple / multiway challange / responce protocol

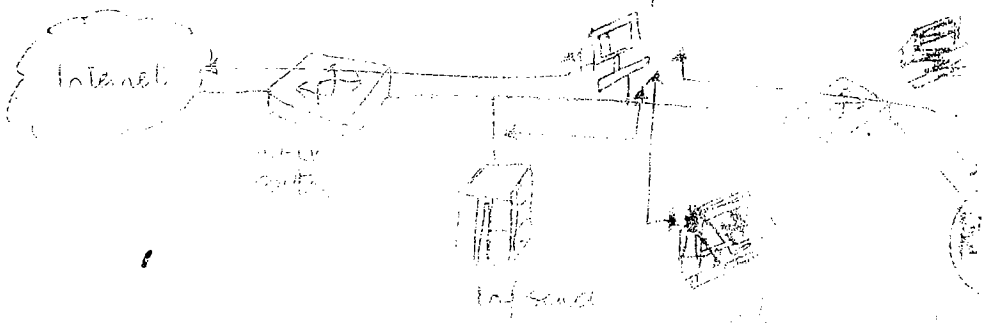
* Kerberos
* Otway - Rees
* Needham - Schroeder



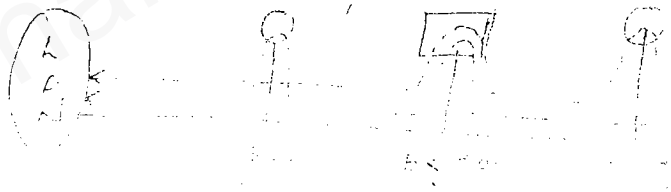
Here Alice encrypt the [illegible] Ra [illegible] with public key of Bob. Then Bob respond to Alice and the challenge generated by A, R_B and a session key. Transfer to authentication Alice respond to Bob by encrypting R_B with the session key.



Components :- two packet filters
2 One AGW



(i) Outside PF and (ii) Bastion.
Outgoing packet is checked by
(i) Inside PF and
(ii) AGW



Supposed to be not an impostes
Mutual Auth } using Public key
+
Key managment }

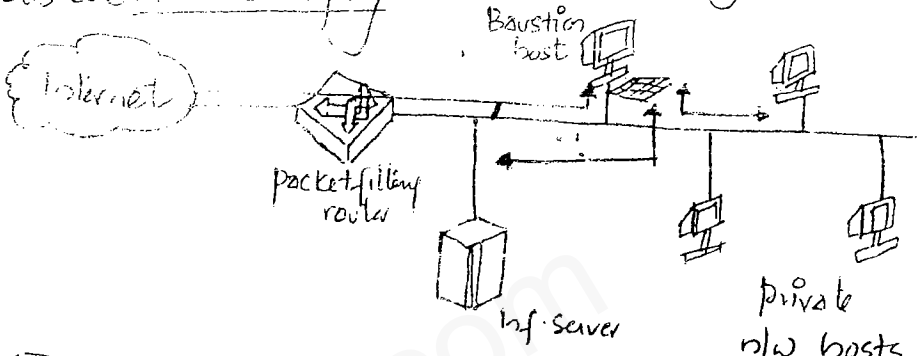
(4) Bastion Host

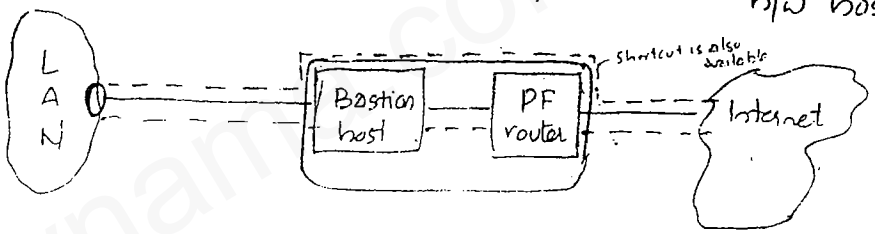
A system identified by the firewall administrator as a critical, strong point in the networks security.

The bastion host services as a platform for an application level or circuit level gateway.

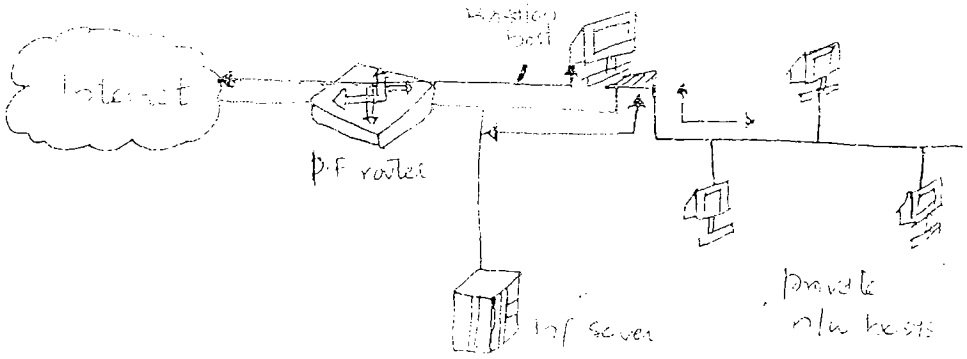
Firewall Configurations

(1) Screened host firewall, single home bastion config





(2) Screened host firewall dual homed bastion host



fragment attack

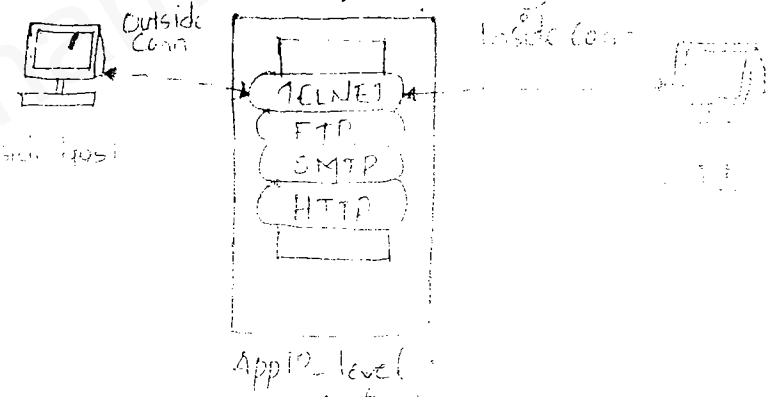
Data that are sent to the destination are sent by a number of fragments

Firewall characteristics

Design goals

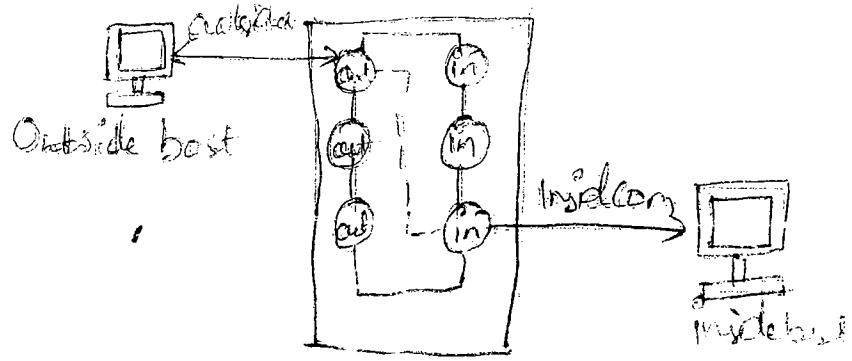
* All traffic from inside to outside must pass through the firewall (by blocking all access to local site except via the firewall)
* Only authorized traffic (as defined by local security policy) will be allowed to pass
* The firewall itself is immune to penetration (use of trusted system with a secure OS)

② Application-level gateway



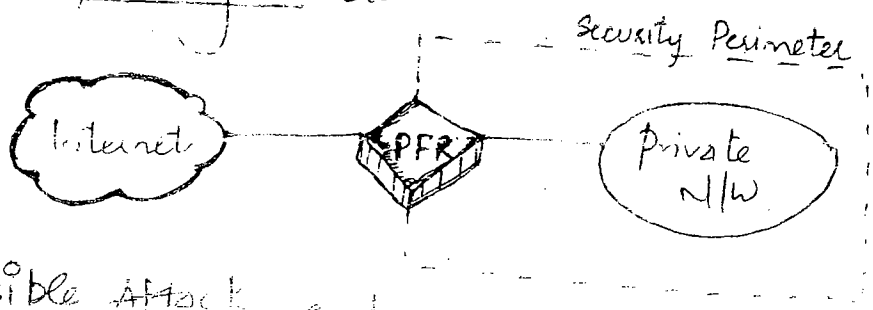
App'n level gateway

③ Circuit level Gateway



Circuit level gateways (CGW)	Packet filter or Screening Router (PF)	Application Gateway (AGW)	Bas... CG... A...
Physical	Network	Application	

① Packet filtering Routers



Possible Attack and Appropriate Countermeasure

Interview Questions

- ✓ SNIFFING
- ✓ SNOOPING
- ✓ SNOOFING
- ✓ PHISHING

Interview
Sniffing

Possible Attack PHARMING

① IP Address – Spoofing
Attacker declares inside n/w's IP address and enter the premises

② Source Routing attack

A B = strict source Route
loose source route
Used to fasten the routing
Packet switching use strict source routing
(i.e Clear route should be provided))

In the RSA Alg. the private and public ke
(d,n) and (e,n) respectively, their
n = p × q and p and q are
Besides
Let M be an integer such that
$\phi(n) = (p-1)(q-1)$

Now consider the following

I) $M' = M^e \bmod n$

$M = (M')^d \bmod n$

II) $ed = 1 \bmod n$

III) $ed = 1 \bmod \phi(n)$

IV) $M' = M^e \bmod \phi(n)$

$M = (M')^q \bmod \phi(n)$

(a) I and II (b) I & III (c) I & IV (d) II & IV

Ans (b)

$P^e \bmod n = C$

$C^d \bmod n = P$

Given $M^e \bmod$

Firewalls

Bad in | Bad Out : stopped

Types

- Circuit level Gateway
- Packet filtering router
- Application gateway
- Bastion host

Extended Euclidean Algorithm

x_1	x_2	x_3	y_1	y_2	y_3	$Q = \left[\frac{x_3}{y_3}\right]$
1	0	z	0	1	d	

$\star = L - Q \cdot R$

eq(1) $(ex1) \bmod 360 = 1$

x_1	x_2	x_3	y_1	y_2	y_3	$Q = \left[x_3/y_3\right]$
1	0	360	0	1	7	$\left[\frac{360}{7}\right] = 51$
0	1	7	1	-51	3	$\left[\frac{7}{3}\right] = 2$
			-2	103	1	

(mul) expat

So Ans is $e = 103$

eq(2) $(5 \times d) \bmod 96 = 1$

x_1	x_2	x_3	y_1	y_2	y_3	$Q = \left[x_3/y_3\right]$
1	0	96	0	1	5	19
			1	-19	1	

Here Ans obtained is -ve so add it with 96

i.e. $(-19 + 96) = 77$

④ $ed \bmod z = 1$

$(ex27) \bmod 96 = 1$

$e = 3$

p	$p^3 \bmod 55$
a=1	$1^3 \bmod 55$
b=2	$2^3 \bmod 55$
c=3	8^3
d=4	4^3
e=5	5^3
f=6	6^3
g=7	7^3
h=8	8^3
i=9	$9^3 \bmod 55 = 14$
j=10	$10^3 \bmod 55 = 10$

Problem 9

$p=7 \quad q=17 \quad e=5$

What is the val of d

① $p=7 \quad q=17$

② $n = 119$

$z = 6 \times 16 = 96$

③ $GCD(d, 96) = 1$

Given $e = 5$

$ed \bmod z = 1$

$(5xd) \bmod 96 = 1$

$\rightarrow (96 \times 4) + 1 \bmod 96 = 1$

$5 \times d = 385$

$d = 77$