NETWORK SECURITY

* Stallings
  forouzan

  A for projects
  Cryptography in 'c'
  Bruce schneier

* GATE SYLLABUS
  - ✓ principles of private & public key cryptography
  - ✓ Digitze signature
  - ✓ firewalls

* Security Components
  1. Confidentiality
  2. Key Management
  3. Authentication
  4. Digitze signature
  5. Compression

* Email Security PGP - pretty good privacy Pem
  Privacy enhanced mail.

1 ✓ ✓
2 ✓ ✓
3 ✓ ✓
4 ✓ ✓
5 ✓ ✓
✓ ✓

Centificlsltially

cryptology   cryptography   cryptanalysis
breaking

Terminology

P = plaintext = data format

C = Cryptic text = ciphertext um double format

E = Enciptercrand Encryption
E(P) = C

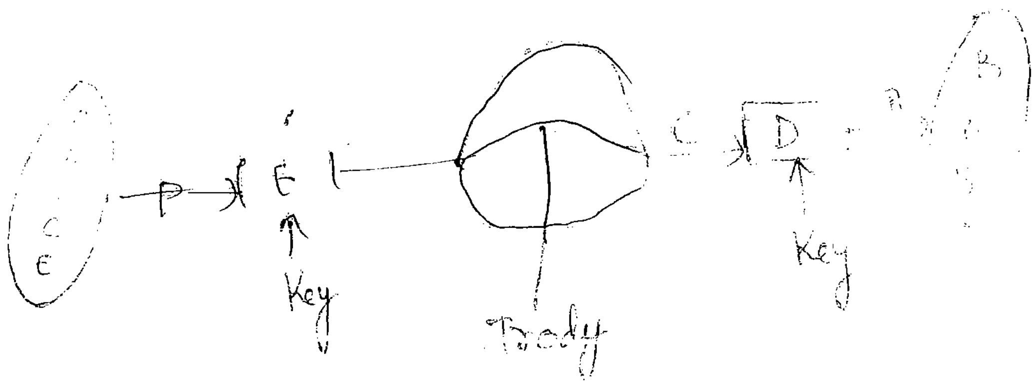
D = Decryption = D(E(P)) = C

So E and D are mutually converse to each other

principle = Comm partners {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 = EDG

② C = LDPDERB

P = ~~IBHDBBX~~

P = I AM A BOY

Approach of Cryptonalyst

Monograms = { I, a

Digrams = { am, an, at, as

{ I ---

Monograms will give clue to digra

Digrams will give clue to Trigr

and so on

Here C = L D P D E R B

k c o c d z a

j b n b c p z

P = I am a Boy

II Substitution Algorithms

a) Monoalphabetic Substitution Algorithm

Ex Mapping Table

a	s
b	u
c	r
d	a
e	n

P = BAD

C = USA

(GOALS) [illegible] even though the plaintext [illegible]
are [illegible]
should not be [illegible] the
world of network security for
the [illegible]
key [illegible]

b) Polyalphabetic substitution cipher [illegible]

Vigenere method

$$\begin{bmatrix} a & b & c & d & e & & & z \\ b & c & d & e & f & - & & za \\ s & t & & u & v & k & & \\ z & a & b & c & & - & - & xy \end{bmatrix}_{26 \times 26}$$

eg: ~~If the egypt~~

corresponding to the plaintext [illegible]
[illegible]
column [illegible] in key) is taken as
is used as ciphertext

(col) key = K [illegible] E

(row) P = S [illegible] S

Even though the ciphertext
letters are repeated the plaintext
letters may not be repeated

(II) TRANSPOSITIONAL METHOD

Plaintext WE ARE DISSCUSSING NWS ~~AT~~ IN ROOM NO # 404

Key = M E G A B V C K

= 7 4 5 1 2 8 3 6

(By numbering as is

M	E	G	A	B	V	C	K
7	4	5	1	2	8	3	6
W	E	A	R	E	D	I	S
S	C	U	S	S	I	N	G
N	W	S	I	N	R	O	O
M	N	O	#	4	0	4	

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

C = RSI#ESN4INC4ECWNAI SGC KISNMDIRO

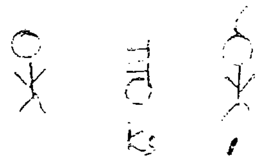
No, of Char received = 31

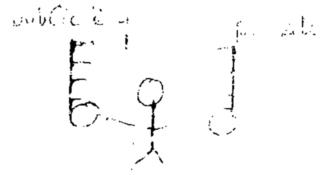
$$8 \overline{)31} = 3, \quad 31 - 24 = 7$$

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

KEY

SYMMETRIC (or) Private Key Cryptography	ASYMMETRIC Public Key Cryptography
(~~Diff~~ Same)	(Different key)





Ks shared key
Session key

Ex: ✓ DES (56 bit)

- Triple [illegible]

✓ IDEA (128)

present AES (128, 192 ...)
(Adv. encry. std)

adv : fast

Disadv : Key Distribution

Ex: i) RSA & MIT
ii) [illegible]
iii) Knapsack

appl ✓ Confidentiality
✓ Key [illegible]
✓ Authentication
✓ [illegible]

Disadv [illegible]

the session key between the sender a[illegible]

$g^{xy} \bmod n = 3^{10 \times 8} \bmod 47$

$= 3^{80} \bmod 47$

$= \underline{4}$

4. The total number of keys required for a set of [illegible] 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	×	✓	✓	✓
2	×	×	✓	✓
3	×	×	×	✓
4	×	×	×	×

Here, 6 key required

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

for public key cryptosystem $2n$

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

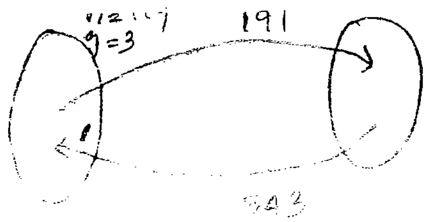
Diffie Hellman key exchange alg. is used. The sender sends (719, 3, 191) and the receiver responds with 543. If the receivers secret key is 15 then calculate the session key.

$n = 719$

$g = 3$

$3^x \bmod 719 = 191$

$3^{15} \bmod 719 = \cancel{191}\ 543$



Session key = $(191)^{15} \bmod 719$

$= \underline{40}$

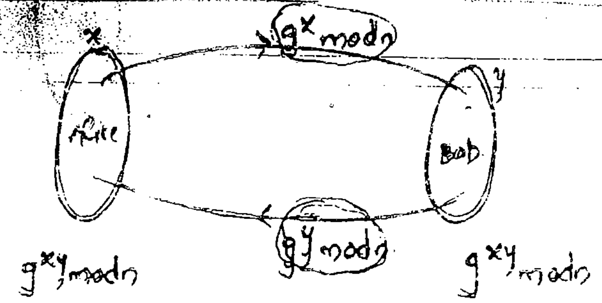
12/11/10
FRIDAY

DATA ENCRYPTION STANDARD (DES)

- Devised @ IBM
- Based on mono alphabetic ... fixed
- ~~Attack~~ = leslie
- proof = fiestel
- 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 MANAGMENT

DIFFIE HELLMAN KEY EXCHANGE ALGORITHM (DH Al...



x - Secret key sender

y = Secret key of Rece...

g^{xy} mod 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

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

② N = 47

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

FAST EXPONENTIAL MODULAR ARITHEMETIC

$M^e \bmod n$

e = expond in binary

Initially d = 1

Untill e' bits exhausted

d = (d × d) mod n

If (b_i = 1)

d = (d × M) mod n

eg: ① $3^8 \bmod 47$

$e=8$	1	0	0	0
$d=1$	1	9	34	28
	3	x	x	x

$= \underline{28}$

② $543^{16} \% 714$

$e=16$	1	0	0	0	0
	1	59	605	54	40
	543	x	x	x	x

$e=15$	1
$d=1$	1
	191

1
40

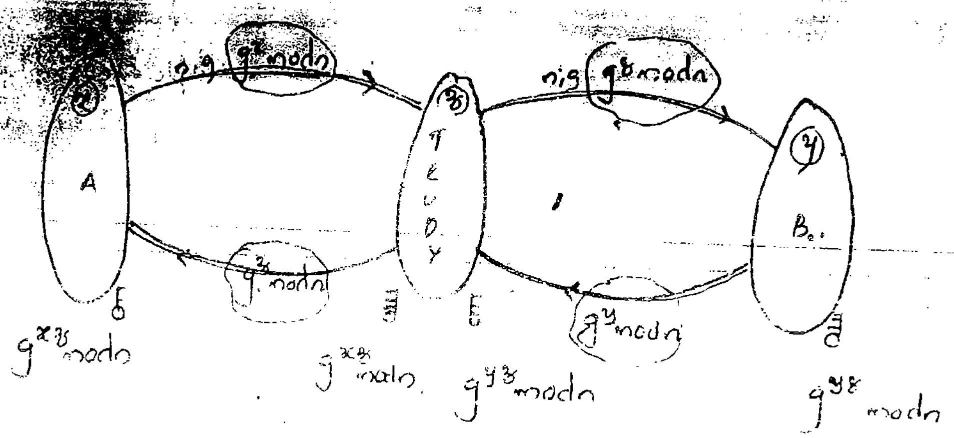
③ $3^{10} \% 47$

$e=10$	1	0	1	0
$d=1$	1	9	34	17
	3	x	8	x

④ $17^8 \bmod 47$

$e=8$	1	0	0	0
$d=1$	1	[illegible]	2	4
	17	[illegible]	[illegible]	[illegible]

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 in 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) $N = 47$

$(N-1)/2 = \frac{46}{2} = 23$ ✓

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 senders 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 $y=35$ and if it responds with the message (____) fill the blank.

$$g^y \bmod n = \cancel{5^3 \bmod 23}$$
$$= 7^5 \bmod 23$$
$$= 11$$

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 Helman key exchange is being used - 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

$$3^8 \bmod 47$$

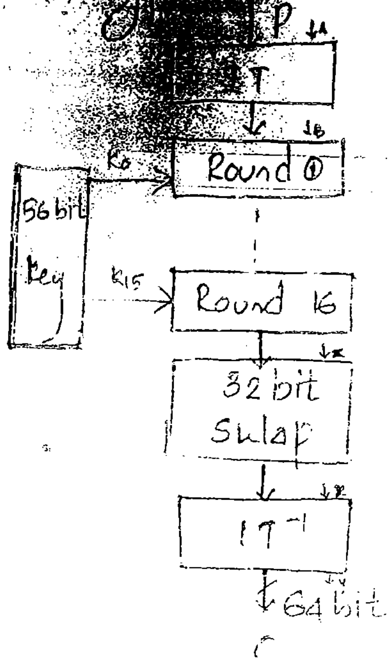
$$= 28$$

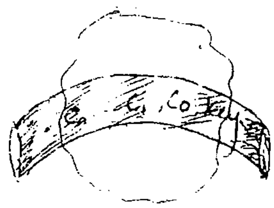
1	0	0	0
1	9	34	28
3	x	x	x

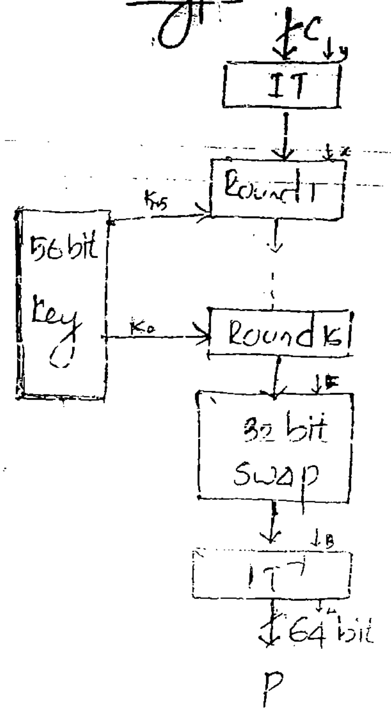
(b) Receiver's secret key $y=10$ and if it responds with the msg (____) fill the blank

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

$$= 17$$

Encryption 



Decryption 

7

Eg: IT

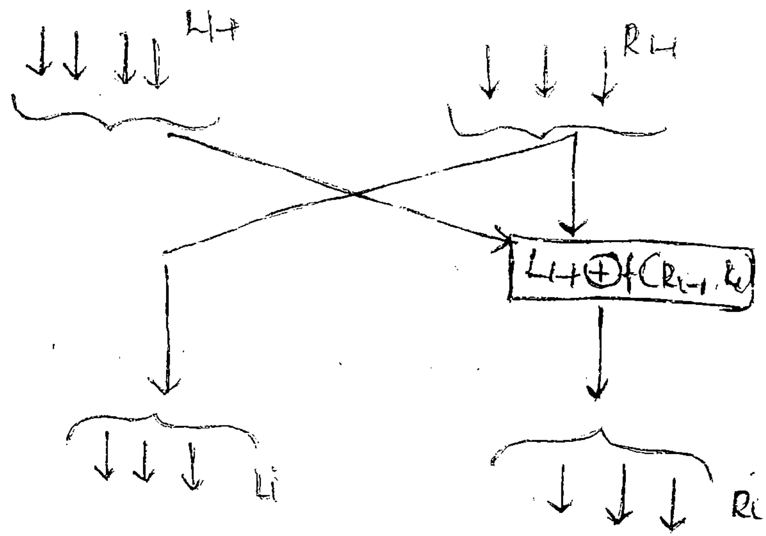
0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6

IT^{-1}

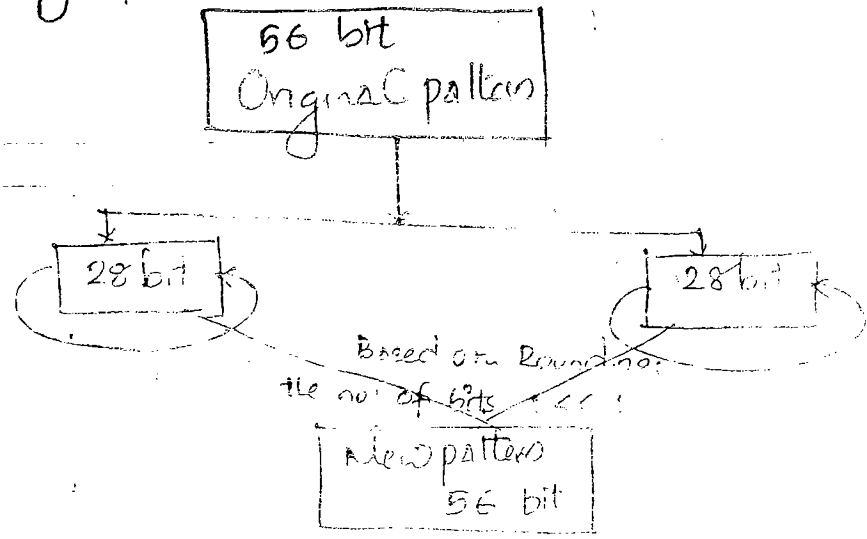
0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6

it is a symmetry

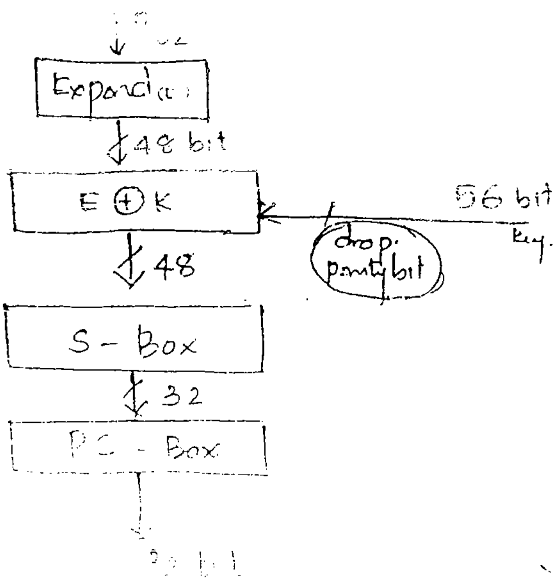
Round



Subkey Generation



f (R, K)



If no:of '1' is odd t
If " '0' is even t

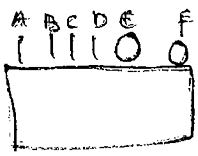
Expand

$8 \times 4 = 32 \Rightarrow 8 \times 6 = 48$

S - Box

AF \ BCDE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00																
01																
10	9	6	F	B	5	D	2	E	A	5	1	8	4	7	0	3
11																

if Input is S box is

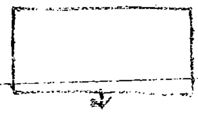


goto AF 10 and look 1 0 in

[illegible]put is 0000

eg.

1 1 0 0 0 0



Here. AF = 10 BCDE = 1000 ie 8

So output of S-box is A = 1010

8.

0	0
1	0
2	
9	
A	10
B	
C	
D	
E	
F	1

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

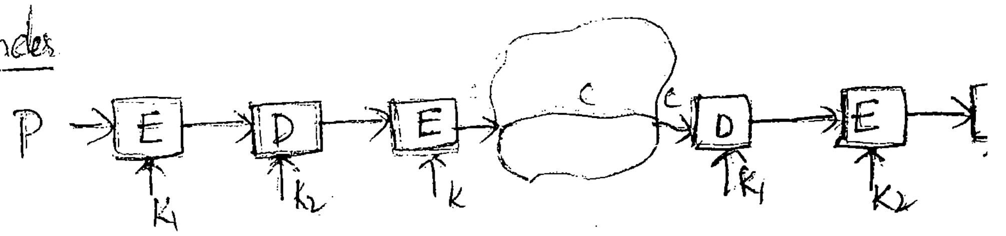
* Encryption with 3 keys

[illegible] 168 bit

* But IDEA has come with 128 bit key only
* So now-a days Triple DES with 2 keys

[illegible] 112 bits

Sender



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

$\rightarrow D_{K_1}(E_{K_2}(D_{K_1}(E_{K_1}(D_{K_2}(E_{K_1}(P))))))$

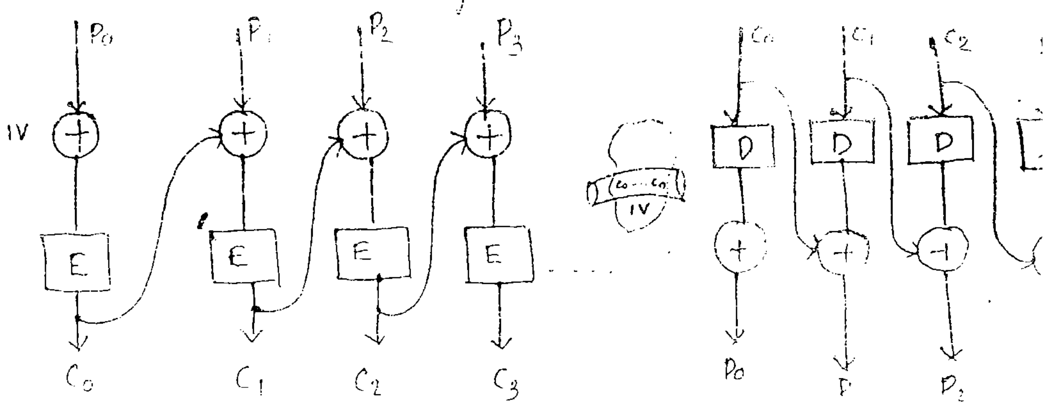
Modes

1) Electronic Code Book Mode

Leslie Attack - Cipher Block chaining

* Manipulation is done on ciphertext and got financially benefited

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



Encryption

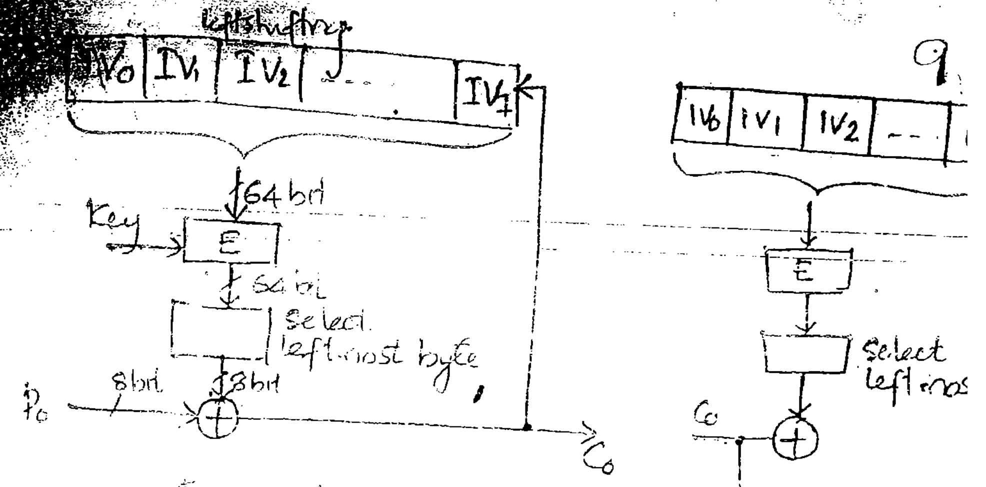
Decryption

* Bit error causes an impact on two blocks only [i-th and (i+1)th block]

* Bit timing error causes the impact on all subsequent blocks [illegible]

Cipher Block feedback mode

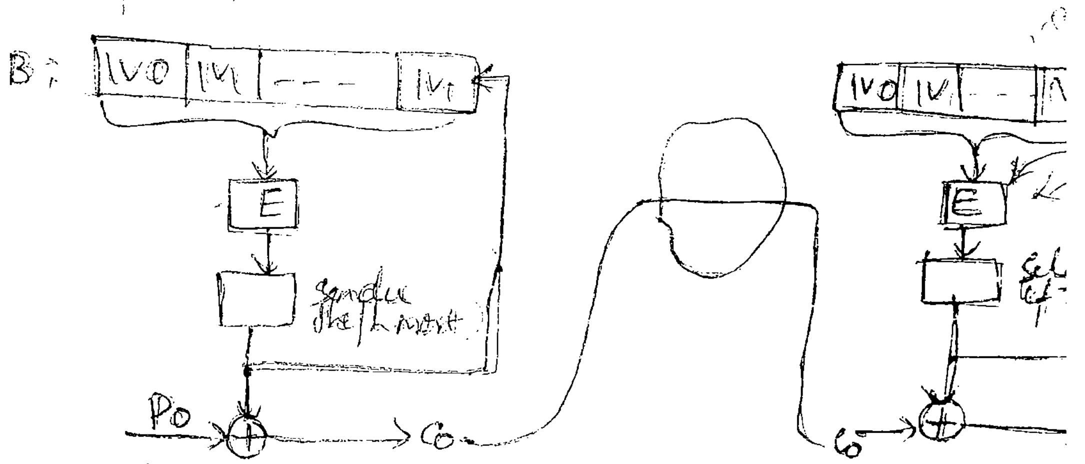
* Used when the input size is less than block size



Encryption   Decryption

* Only $\boxed{E}$ box in 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[tes] 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

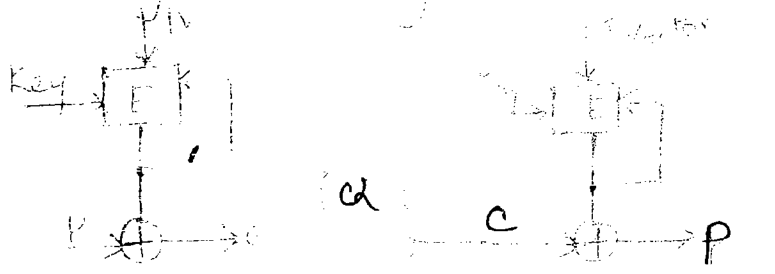


* Let ith byte error should not cause its impact on subsequent bytes, so the feedback is considered from the o/p end

This mode is not robust ~~becoz~~ cryptanalyst Can easily break this since it works on the cyclic data

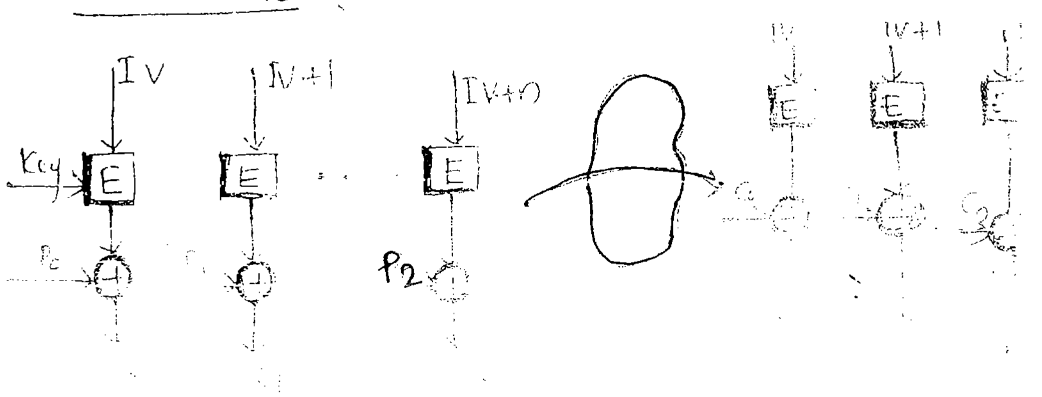
5. Stream Cipher

when the [illegible] (bit stream), then selection [illegible] required well in advance the third [illegible] data must have encrypted [illegible] readily waiting for the [illegible] stream



Encryption Decryption

6. Counter Mode



→ Now a days the database data [illegible] the [illegible] cipher text

→ Not to depend on the preceding second C to decrypt the individual (second) Counter is attached. The Counter will be all No SSN PAN Card No or any Unique identifier

Modes is practice real world

input

[diagram in booklet]

(iv) e° R

Large size — chaining is used (ii)

< block size — feed back is used (iii)

(v)

(vi)

13/10/10 SATURDAY

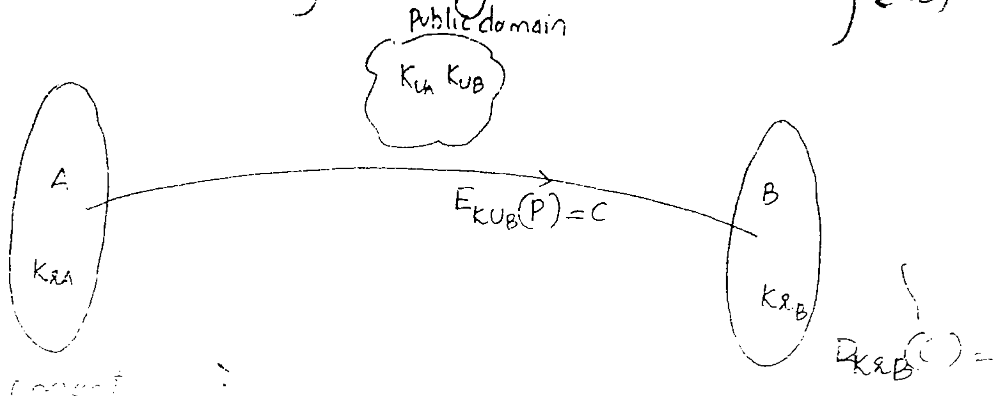
PUBLIC KEY CRYPTOGRAPHY

Assymmetric Key Alg

Two keys

↳ One Key = Encryption = public key (K_u)

Other Key = Decryption = private key (K_R)



Requirement :

* [illegible] keys are diff The above conclusion is possible just because both keys are originated by the same one

$D_{KRA}(E_{KUA}(P)) = P$

* One cannot guess (D_k {K_R} private key) from known public key (E or {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 [illegible] relatively prime [illegible] and call it d
4. Find e such that $e \times d = 1 \bmod z$

$$ed \bmod z = 1$$

Encryption $K_U = \{e, n\}$

$$p^e \bmod n = C$$

Decryption, $K_R = \{d, n\}$

$$C^d \bmod n = p$$

Eg. (1) p = [illegible] q = 11

(2) $n = 3 \times 11 = 33$

(3) $z = 2 \times 10 = 20$

(5) [illegible]

Say

(4) $(e \times 7) \bmod 20 = 1$

$21 \bmod 20 = 1$

$e \times 7 \bmod 20 = 1$

$e = 21/7 = 3$

Ans Both are true.

3 The minimum +ve 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 $m = 3$, $e = 12$, $n = 17$

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

5 Diffie Helman keyexchange is being used to establish a session key b/w the sender & the receiver with the values of $n = 23$, $g = 7$.

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

$7^3 \bmod 23 = 21$

(b) Receivers secret key $y = 6$. He responds with the msg —

$7^6 \bmod \ldots = 4$

(c) What is the session key b/w sender & the receiver

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

$= \underline{18}$

$M = 7$, $e = 18$, $n = 23$

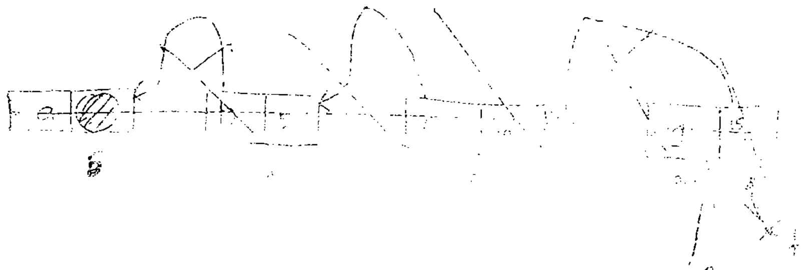
$e = 18$

$d = 1$

1	0	0	1	0
1	3	9	12	18
7	X	X	15	X

a SLC

QUESTIONS



1 Suppose that two parties A & B wish to settle a common secret key b/w themselves using diffie Helman key exchange tech. They agree on 7 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 ...

$n = 7$ $g = 3$ $x = 2$ $y = 5$

$g^{xy} \bmod n$

$=$

2 Consider the following two statements

(i) ...

... performs a permutation on the elements of its input alphabet

Ans

bijective function means only one function have only one mapping. No Not function can map to one

6. The RSA Alg. is used by choosing two prime no: 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

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	$q = 19$
0	1	5	1	−19	1	

$96 + \cdot 19 = \underline{\underline{77}}$

②

$p = 6$

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

7 RSA alg is used with prime no: 397 & 401 to generate public keys & private keys.
① If the e is choosen as 343 then calcu 'd' value

$(343\, d)$

$(343\, d)$

x_1	x_2	x_3	y_1	y_2	y_3	$q = \left[x_3 / y_3 \right]$
1	0	158400	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	

$d = \underline{\underline{12007}}$

(8) Diffie Hellman key exchange alg. is used ... sends $(7, 3, 7^3 \bmod 23)$ and the receiver responds with $(7^6 \bmod 23)$ then calculate the session key

$7^{18} \bmod 23$

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

Ans - 18

(c) $a = 18$

$d = 1$

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

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

5 words of 32 bits. 5×32 160

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

I The receiver can verify the claimed ...

II ...

III The receiver cannot possibly have concocted the msg. himself

Ans I II & III

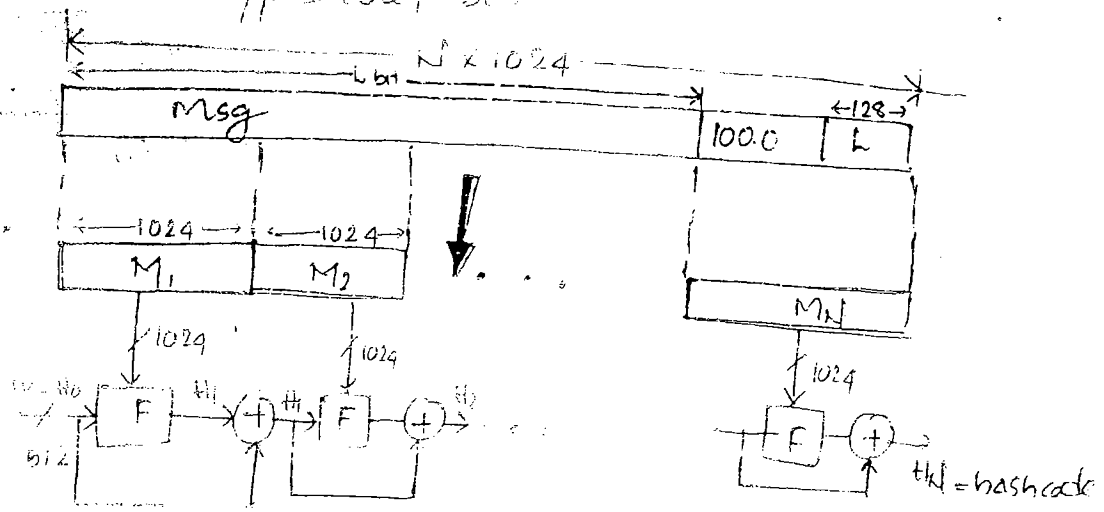
(11) Diffie Hellman key exchange ... the sender sends ... and the receiver responds with 543 if the receiver secret key is ... the calculate the session key

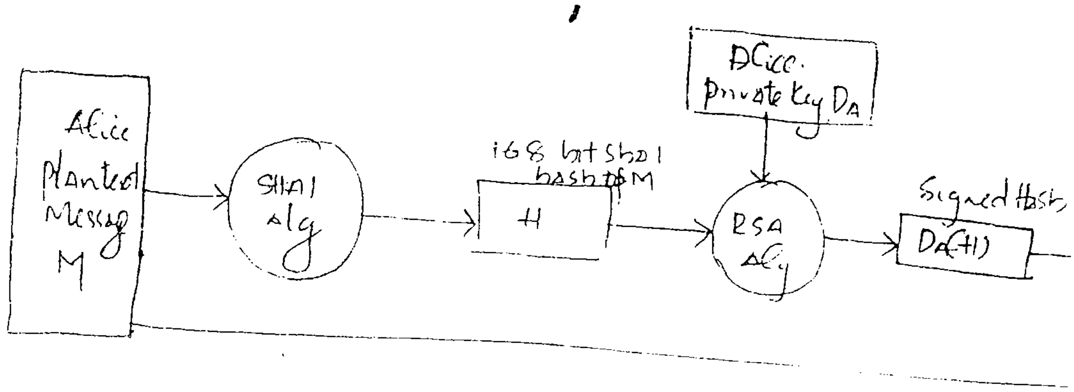
Observation

sha-512

o/p = 512 bits

i/p = 1024 bits





Observation

1) we Do encryption first then zip

1000 → [E] → 1000 → [zip] → 100

2) we are doing zip then encryption

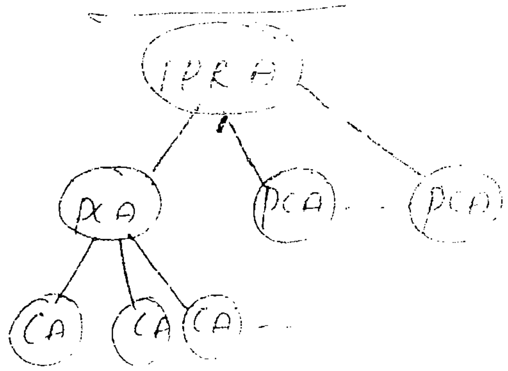
1000 → [zip] → 100 → [E] → 100

Second is fast because only 100 bits are need to encrypt

Email Security

~~Devised by~~	PGP (Pretty Good privacy)	PEM [illegible]
Devised by	Phil ~~IDEA~~ Zimmermann	[illegible]
Confidentiality	IDEA	[illegible]
Key mgmt	RSA / Haphazard	RSA / IPRA
Auth & Digital Sig.	RSA + MD5	RSA + SHA-[illegible]
Compression	[illegible]	

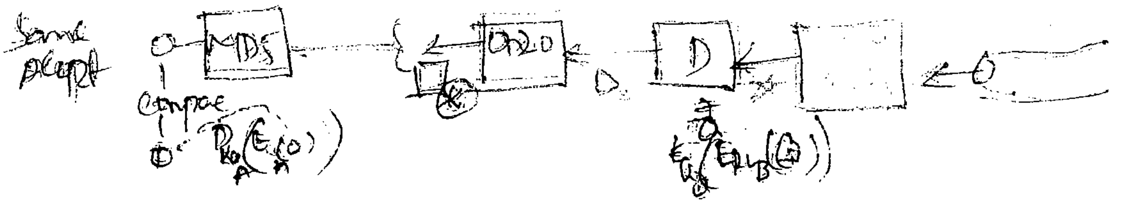
IPRA (Internet Policy Registration [illegible] Auth



PCA - [illegible] Certifi

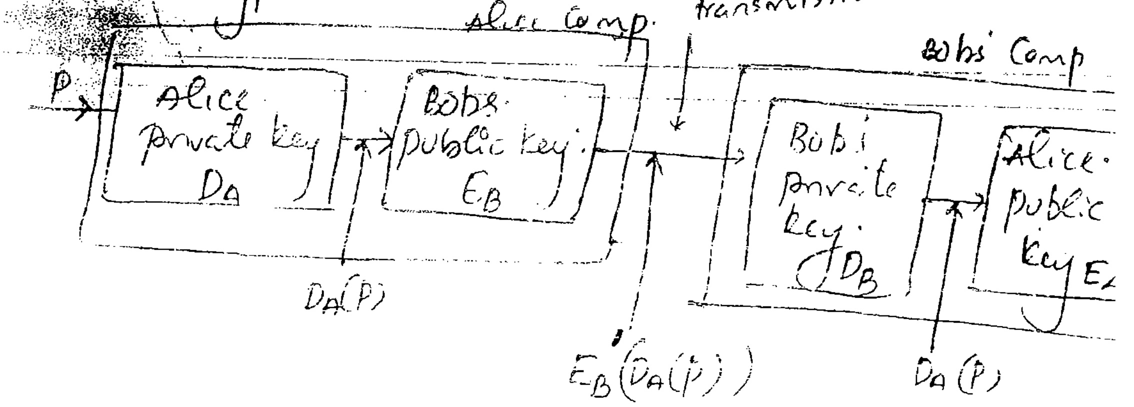
CA - Certificate Authori

Certificate (x.509) = Ku + Ke + additional



E = Encryption = Ku

D = Decryption = Kr



Message Digests Alg ~~(MD5)~~

~~MD5~~ ~~SHA~~

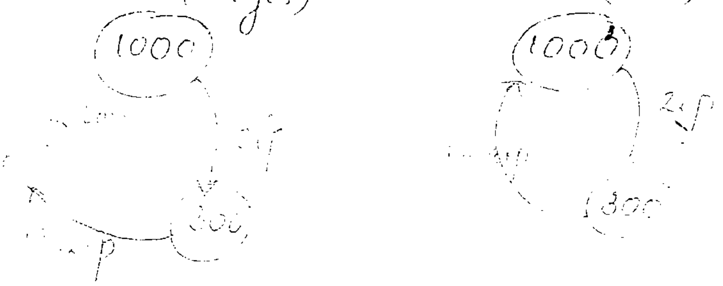
Digest

→ One Way

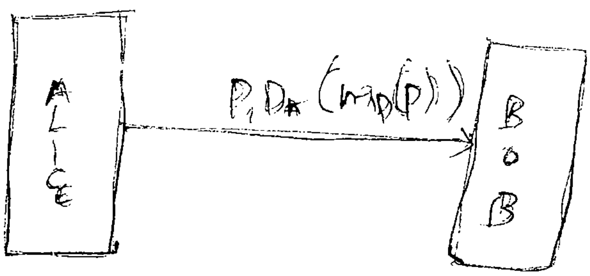
→ The other way is ~~doge~~ impossible
(One directional)

Compression → Bidirectional

Loss (Images)   Loss Less (Text)



MD5



MD5	SHA1
Message digest version 5	Secure hash alg.
o/p = 128 bits	o/p = 160 bit
I/p = 512 bit	I/p = 512 bit
ABCD = 4 register	ABCDE = 5 register
each = 32 bit	each = 32 bit
4 x 32 = 128	160

- Given p it is easy to compute
- Given (P) is effectively impossible to find p
- Given p one find p' such that $MD(p') = MD(P)$
- A change to the length of even 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

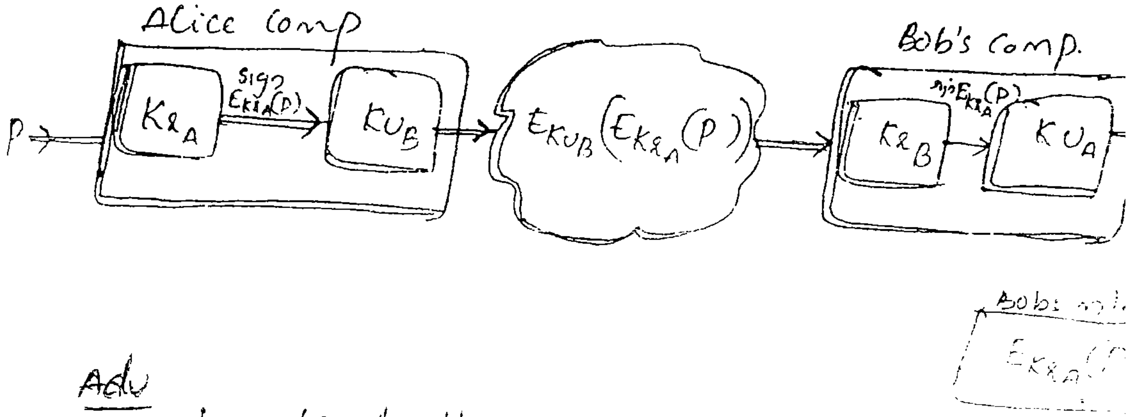
padding bit are append only to make the bits a multiple of 512

Transmission overhead - If msg is 1MB for every encrypted msg, the big signature has to be sent so transmission overhead

2004 Gate Q. Confidentiality : A sender is employing PKC for sending a $\boxed{\text{secret msg}}$ to receiver sender uses receivers $\boxed{\text{public}}$ key

2004 Gate Q. Digital signature: A sender is employing PKC for sending a $\boxed{\text{signed msg}}$ to the receiver & sender uses his/her own [pri] key

DIGITAL SIGNATURES USING PUBLIC KEY CRYP.



Adv
* No big brother
* No transmission overhead

with private key of A & public key of B here message is encryp[ted]

Disadv
* memory overhead is there ie high m/m to store the signature

DIGITAL SIGNATURE

Requirements

* The Receiver can verify the [illegible] identity of the sender [illegible]
* The sender cannot later [illegible] contents of the message
* The receiver cannot possibly [illegible] the message himself

Protocol

Digital signatures with Big Brother

BB = Bigbrother = trusted [illegible]

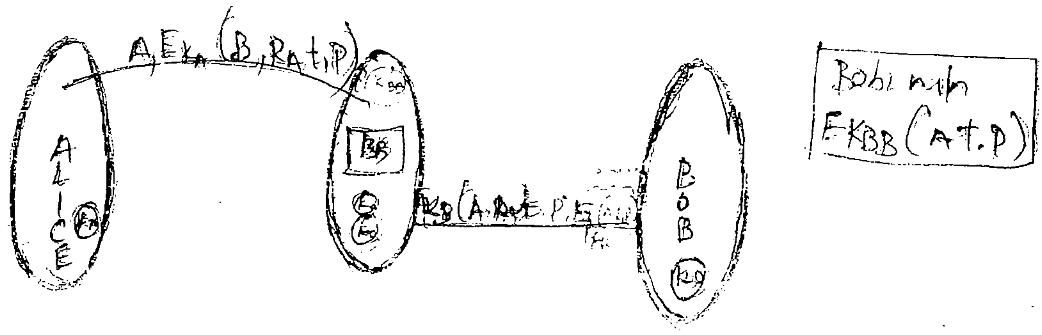
K_{BB} = Secret key with BB used for signature

K_A = Shared key b/w A and BB

K_B = Shared key b/w BB [illegible]

t = time stamp } Not to have [illegible]

P = Nonce



Disadv

1 What if BB ? ! ! !

2 Transmission overhead } Sign is Big

3 Memory overhead

First two handshakes: using ~~pre~~ [illegible]

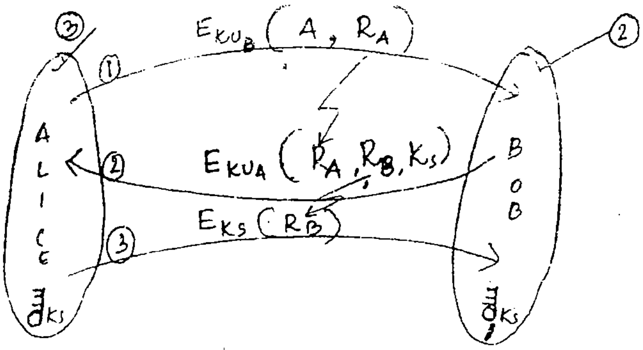
The third handshakes : using symmetric [illegible]
(same key)

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

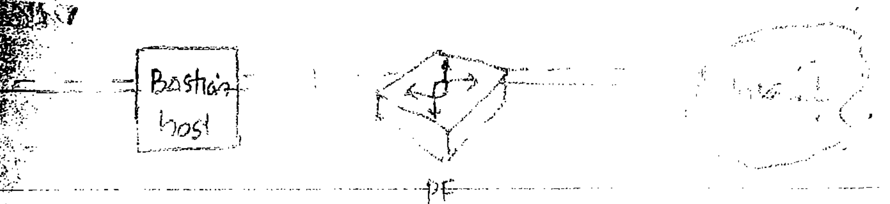
K_s = shared key / session key.

Multiple / multiway challange / responce protocol

* Kerberos
* Otway - Rees
* Needham - Schroeder

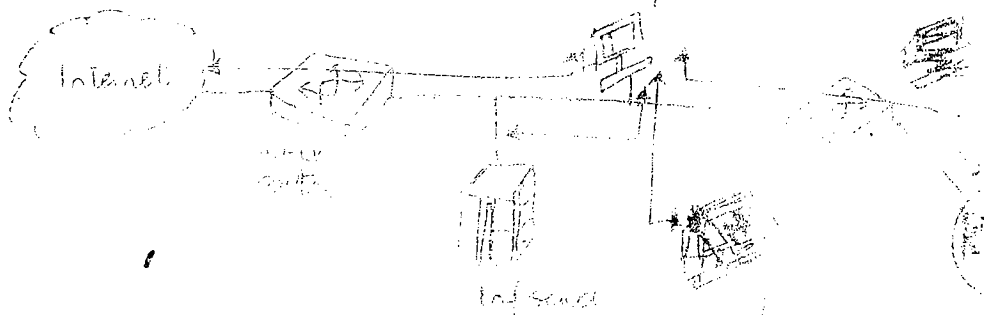


Here Alice encrypt the ~~[illegible]~~ ~~[illegible]~~ ~~[illegible]~~ ~~[illegible]~~ R_A & A with public key of Bob. Then Bob respond to Alice with the challenge ~~and~~ generated by A, ~~and~~ R_B and a session key. In order to authentication Alice respond to Bob by encrypting R_B with the session key.



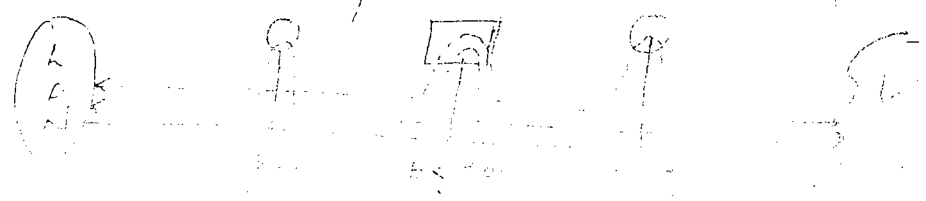
Screened subnet firewall system (a...

Components 1. Two packet f...
2. One AGW ...



(i) Outside PF and (ii) Bastion

Out going packet is check.d by
(i) Inside PF and
(ii) AGW



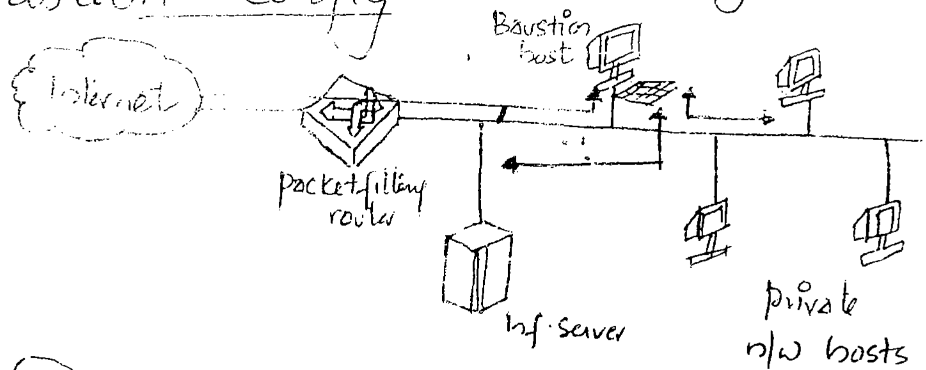
Supposed to be Not an imposter
Mutual Auth + Key managment. } using Public Key

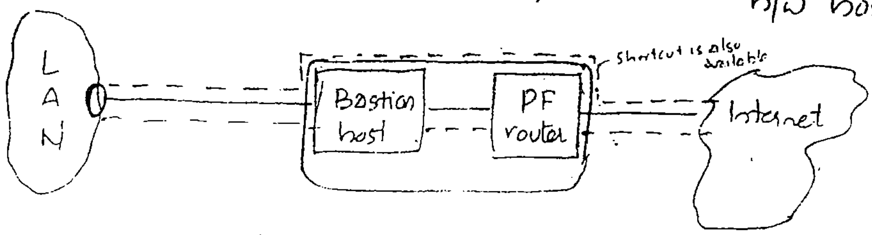
(4) Bastion Host

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.

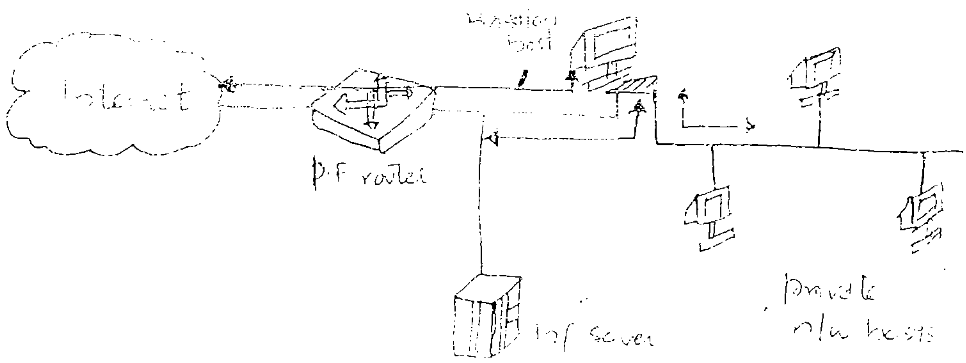
Firewall Configurations

(1) Screened host firewall, single home bastion config





(2) screened host firewall dual homed bastion host



③ fragment Attack

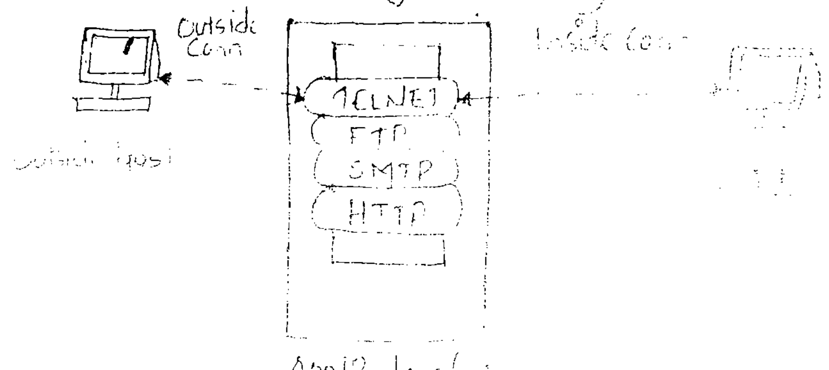
Data that are sent to the destination are sent by a [illegible] fragments

Firewall characteristics

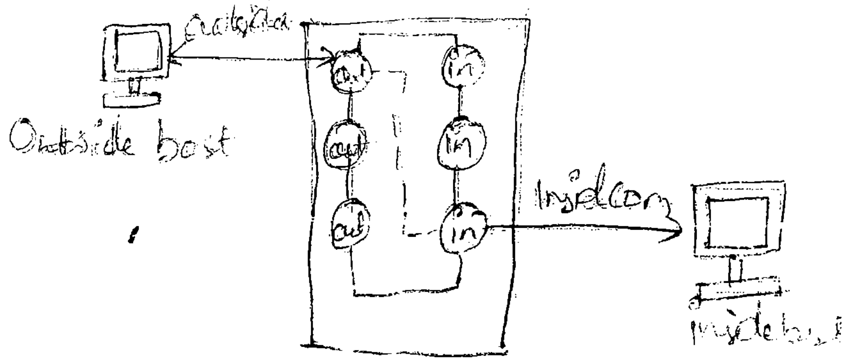
Design goals

* All traffic from inside to [illegible] pass through the firewall (physically blocking all access to local [illegible] except via the firewall)
* Only authorized [illegible] (defined by local security police) will be allowed [illegible]
* The firewall itself is immune to penetration (use of trusted s/m [illegible] secure OS)

② Application-level gateway

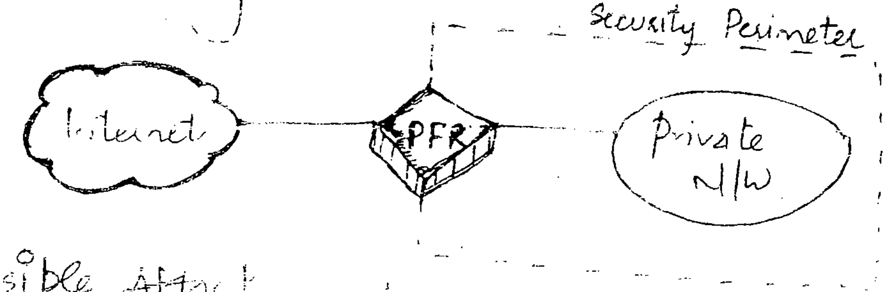


③ Circuit level Gateway



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

① Packet filtering Routers



Possible Attack and appropriate Countermeasure

Interview Questions

~~Interview Sniffing~~

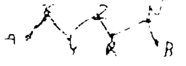
- ✓ SNIFFING
- ✓ SNOOPING
- ✓ SNOOFING
- ✓ PHISHING
- ✓ PHARMING

Possible Attack

① IP Address – spoofing

Attacker declares inside n/w's ip address and enter the premises.

② Source Routing Attack



= Strict Source Routing

Loose Source routing

In order to fasten the routing

packet switching use strict source routing (ie Clear route should be provided))

Q) [illegible] the RSA Alg. the private and public ke[illegible]
[illegible] (d,n), and (e,n) respectively, where
$n = p \times q$ and p and q are large primes
Besides n is public, p and q are pri[illegible]
Let M be an integer such that $0 < M < n$

$\phi(n) = (p-1)(q-1)$

Now consider the following [illegible]

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

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

II) $ed \equiv 1 \bmod n$

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

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

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

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

Ans (b)

$p^e \bmod n = c$ | Given $M' = M^e \bmod$ [illegible]

$c^d \bmod n = p$

Firewalls

Bad in | Bad Out : stopped

Types

- ✓ Circuit level Gateway
- ✓ packet filtering routers
- ✓ Applnlevel gateway
- ✓ Bastion host

Extended Euclidean Algorithm

x_1	x_2	x_3	y_1	y_2	y_3
1	0	z	0	1	d

$Q = \left[\frac{x_3}{y_3}\right]$

$\boxed{\star = L - Q \cdot R}$

Eg(1) $(e \times 7) \bmod 360 = 1$

x_1	x_2	x_3	y_1	y_2	y_3
1	0	360	0	1	7
0	1	7	1	-51	3
			-2	$\boxed{103}$	1

$Q = \left[x_3 / y_3\right]$

$\left[\frac{360}{7}\right] = 5$

$\left[\frac{7}{3}\right] = 2$

(add) repeat

So Ans is $e = \underline{103}$

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

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

Here Ans obtained is $-ve$ so add it with y

i.e. $(-19 + 96) = \underline{77}$

④ ed mod $z = 1$

$(e \times 27) \bmod 40 = 1$

$e = 3$

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

Problem 9

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

what is the VAC 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 mod $z = 1$

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

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

$5 \times d = 385$

$d = 77$