LEARNING UNIT 3

Security of E-Commerce

Transactions between organizations take place in many e-commerce applications using the Internet. Internet is widely accessible and insecure as eavesdropping is possible. Hence, there is need to protect company confidential information from snoopers.

We also need to protect a company's network from unauthorised entry. When an organization receives a message it has to be sure from whom it came and whether the message is authentic and not changed by an unauthorised person. We thus need a digital signature which can be used in a court of law.

Network Security Using Firewall

Firewall is a security device deployed at the boundary of an organization' s network to protect it from unauthorised external access. It links an organization's intranet to the internet and restricts the type of traffic that it will pass, thus providing security. Simple firewalls may be implemented in some routers, called packet filtering firewalls, they pass only some packets based on simple specified criteria such as

-Type of access (such as email, ftp, telnet as determined by TCP port number)
-Direction of traffic
-Source or destination IP address
-Time of day

Proxy Application Gateway

Proxy application program running on a firewall machine is the one which acts on behalf of all members of an organization wanting to use the internet. This program monitors all requests - allows access to only designated addresses outside, limits use of certain browsers and disallows use of some protocols with known security holes. Proxy application program may also be allowed to run on some user's machine who have authorization for internet use.

Hardened Firewalls With Proxy Application Gateway

Any one from inside or outside an organization give their user id, password, service required to the firewall machine which acts as one's proxy (ie.does ones work on his behalf). Proxy firewall is now server to the requestor's desktop PC and also a client to some other requested service acting on requestor's behalf. Firewall needs proxy agent for each service requested such as FTP, HTTP, TELNET etc. Now proxy firewall is the initiator of all sessions and thus knows every activity - thus ensuring security. Firewall with a proxy function replaces the source address of transaction requestor with its own IP address

-this ensures that others on internet see only firewall's IP address - all other IP addresses of organization are hidden

Data Encryption With Secret Keys

Data sent via a public network may be accessed and used by unauthorized persons. Thus it is necessary to scramble it so that even if one accesses it, it cannot be understood. Similarly data stored in data bases accessible via internet should be scrambled. Method of scrambling is known as encryption. Method of unscrambling is known as decryption.

Plain Text And Ciphertext

•Plain text is data in its natural form

•Encryption is taking data in any form(Text, Audio,Video etc.) and transforming it to another form which cannot be understood

•Transformed data is known as cryptogram or cipher text

Example Text Encryption

Start plaintext	THIS IS A MESSAGE X
Block plaintext (5character blocks)	THISI SAMES SAGEX
	4➪1
Transpose characters with permutation (4 1 2 5 3)	STHII ESASM ESAXG
Substitute character by the one 4 letters away (eg A➪E,Z➪D)	WXLMM IWEWQ IXEBK
	Cipher text

This is an example of two transformations - permutation followed by substitution
The keys are permutation function and substitution function

Symmetric Encryption

PLAINTEXT (m1,m2…mn)
CIPHER TEXT (c1 c2, c3….cn)Where ci = k(Ti (mi)) In which T**i** is permutation of ith character and k is substitution.
Decryption by applying same transformations in reverse on cipher text. This method called symmetric key encryption as encryption and decryption performed using same key. Normally the encryption/decryption algorithm is publicised. Only key is secret. Problem is to ensure secrecy of key when it is sent to partner. If the key is to be sent to many partners need for separate key for each partner. Directory of who was sent which key is to be kept and used for each transaction. Directory should be secure. If large number of partners are there key distribution becomes very difficult. Advantage of symmetric key is easy and fast to transform plain text to cipher text.

Digital Encryption Standard

DES - Proposed by IBM in 1975
Standardised by US Govt in 1977
It is a combination of permutation and substitution on blocks of 64 bits. A message is broken up into 64 bit blocks and each block is separately encrypted.

#General idea used in DES

M = PLAINTEXT	01101100	11011000	11011010
K=KEY	10101111	00101100	01011011
$E= M \oplus K$	11000011	11110100	10000001 encryption
$M= E \oplus K$	01101100	11011000	11011010 decryption

Digital Encryption Standard Algorithm

Before applying DES the text is split up into the 64 bit blocks.
DES applied on each 64 bit block.

Encryption method

Step 1: Apply an initial permutation on a block.Result is B=IP(P) where P is the 64 bit block IP Initial Permutation function and B the result.

Step 2: Split B into 32 bit blocks
Li = leftmost 32 bits
Ri = rightmost 32 bits.

Step 3: Pick a 56 bit key. Permute it

Step 4: Left circular shift it by 1 bit giving K1.

Step 5: Perform a complex sequence of operations and obtain X1 = F(R1,K1) (The complex set of operations include table look up and dropping bits).

Step 6: Find R2 = L1 + X1

Step 7: Set L2 = R1

Repeat steps 2 to 7 16 times to get B16 = L16,R16

Step 8: Apply inverse of initial permutation on B16

The result is the encrypted block

In summary the DES encryption applies the following transformation 16 times.

The i_{th} round transformation are

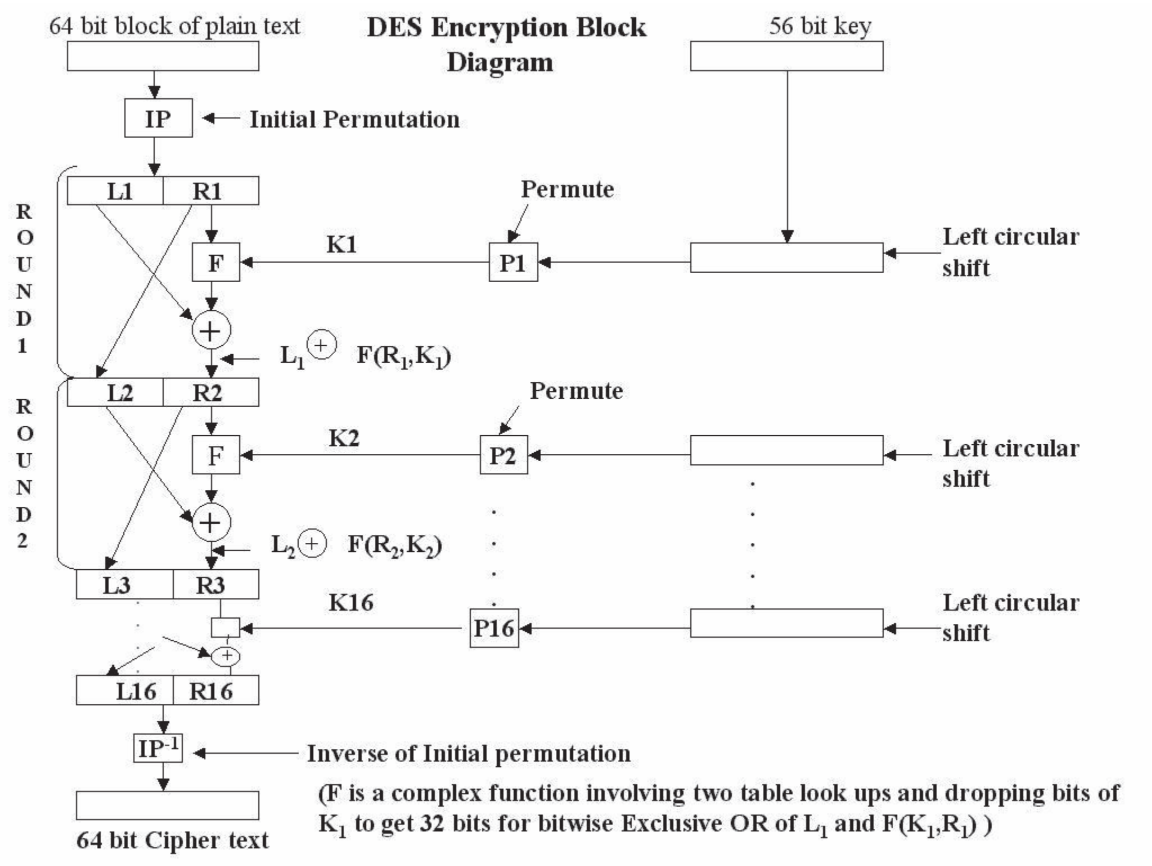
$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i,K_i)$$

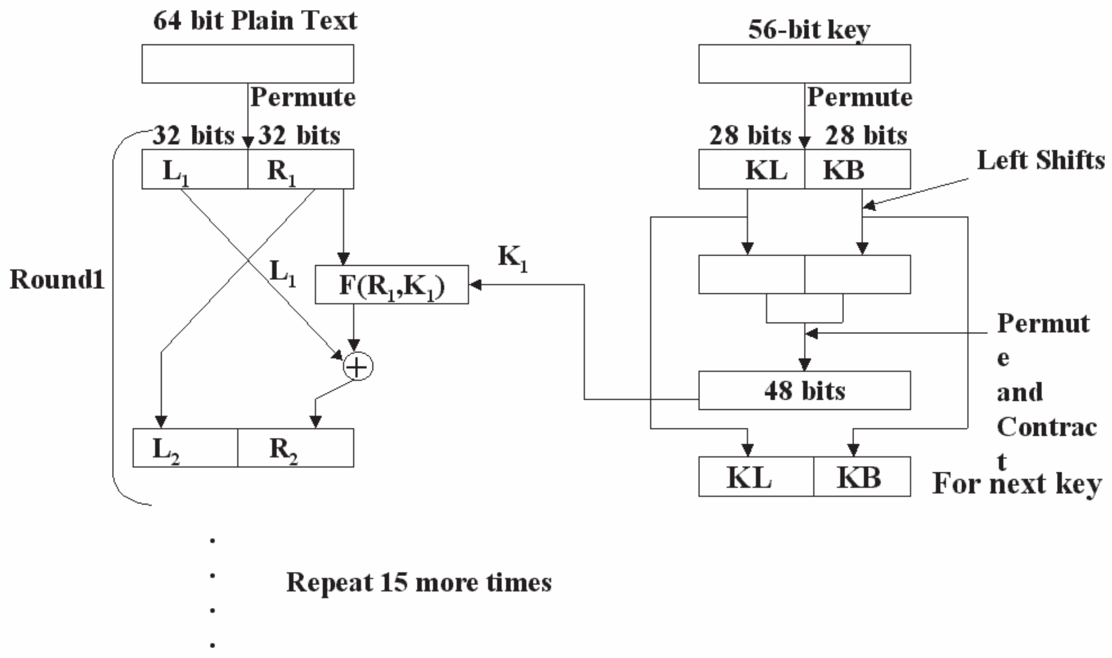
Each round has a different key K_i

For Decryption the process of encryption is reversed. The encrypted block is permuted using IP_{-1}.On this transformations are applied starting with K_{16} and going to K_1 last. The keys and F are same as those used in encryption process.

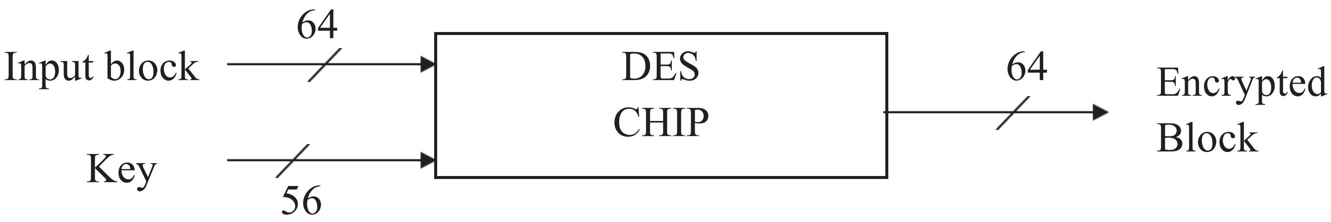
The encryption process uses simple binary operations. They can thus be realised in hardware as an integrated circuit chip. DES chips are inexpensive. Key is externally fed.


64 bit block of plain text
DES Encryption Block Diagram
56 bit key
IP
Initial Permutation
L1
R1
Permute
ROUND 1
K1
F
P1
Left circular shift
L1 ⊕ F(R1,K1)
L2
R2
Permute
ROUND 2
K2
F
P2
Left circular shift
L2 ⊕ F(R2,K2)
L3
R3
K16
P16
Left circular shift
L16
R16
IP-1
Inverse of Initial permutation
(F is a complex function involving two table look ups and dropping bits of K1 to get 32 bits for bitwise Exclusive OR of L1 and F(K1,R1))
64 bit Cipher text

Details of One Round of DES Encryption



DES Chip



Observe that from initial key others are derived by circular shifts
Decryption chip inputs encrypted block and key and the output is decrypted block

DES - Discussion

Cryptananalysis is technique for breaking a code, given the samples of encrypted messages. If plain text also known it is somewhat easier. DES code can be broken if key is found. The easiest method of breaking a code is by brute force of trying out all possible keys to decrypt message. With increase in speed of computers it has now been shown that DES key can be found in less than 12 hrs with a fast computer (1 Million decryption per microsecond). Thus DES is practically useless now (original DES was invented in mid 70s). New more secure symmetric encryption algorithm is needed. An extension of DES called triple DES is shown to be more secure.

Triple DES

Triple DES uses three different keys and three executions of DES algorithm.

The algorithm is

Cipher text = $E_{\mathbf{k3}}$ [$D_{\mathbf{k2}}$ [$E_{\mathbf{k1}}$ [Plain Text]]]

where $E_{\mathbf{k}}[X]$ = DES Encryption of X using key K

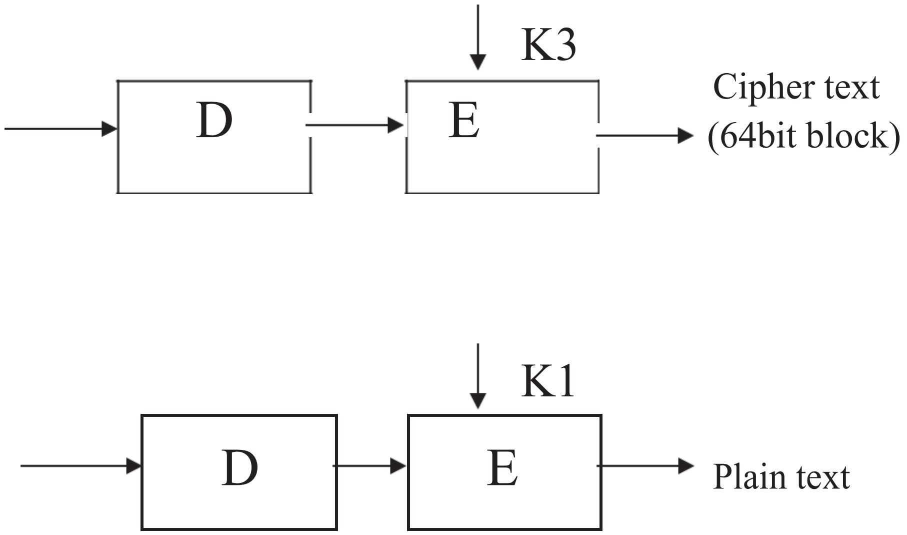
and $D_{\mathbf{k}}[X]$ = DES Decryption of X using key K

Remember that in DES Decryption of encrypted plain text with a different key is almost same as another encryption. This is true as encryption and decryption use the same algorithm.

To decrypt cipher text we reverse the operations.

Plain text = D_{k1}[E_{k2} [D_{k3}[Cipher Text]]]

BLOCK DIAGRAMS OF TRIPLE DES



Using DES thrice is equivalent to having a DES key length of 168 bits. Brute force method to break triple DES with 10^{6} decrypts per micro second will take 5.9 X 10^{30} years! Even at 10^{12} fold increase in computer speed will make triple DES secure against brute force attacks to break code

The only reason D is used as middle step in triple DES is to allow decryption of data encrypted using single DES hardware. In this case K3=K2=K1 (Single key used) (See block diagram)

Triple DES will be quite popular for a foreseeable future as it is very secure, can be realised by simple hardware. Triple DES has two disadvantages

1. It is slow to implement in software
2. It uses 64 bit blocks.

Thus new standards were explored.

Requirements of Symmetric Key Cryptography Algorithm(NIST) – Advanced Encryption System(AES)

• National Institute for Standards Technology put out a call for proposals for new crypto system with following requirements.

• Must provide a high level of security (i.e. difficult to decrypt in finite time)

• Must be completely specified and easily understood.

• Security must reside in key – Not in algorithm

• Must be available for all users

• Adaptable for use in diverse applications e.g.credit cards

• Implementable economically in electronic devices

• Must be efficient to use as both software and hardware

• Must allow one to validate it.

• Must be exportable

• No trap door

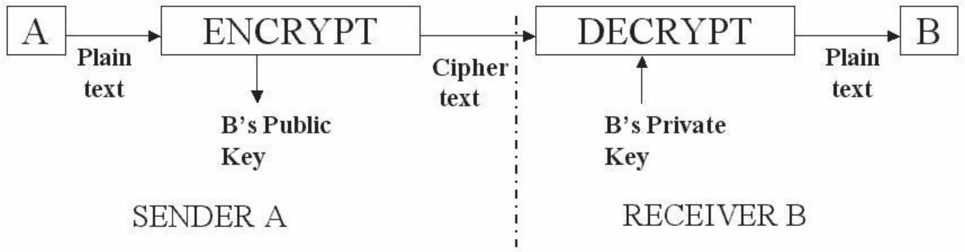
• Must use 128 blocks and key lengths of 128,192 or 256 bits depending on the level of security desired.

• In October 2000 it announced the selection of an algorithm – called Rijin dael(Pronounce RAIN DOLL) as new Advance Encryption Standard (AES)

•Details may be found in www.nist.gov/aes

Public Key Encryption

In Private Key Encryption transmission of key without compromising not easy. It is necessary to assign different private key to each business partner. When this is done a directory of keys should be kept which should be secret. This is difficult. Only secure way is to change the private key every time a message is sent. Public Key Encryption eliminates the key distribution problem. There is a pair of keys for each organization - A Private Key and its Public Key. If A wants to send message to B, A encrypts the message with B's Public Key When message is received by B he decrypts it with his Private Key .



RSA Code Details."R" Wants To Find His Public And Private Keys

1. Pick large primes p and q. Let n =p * q
2 Find ø = (p-l)*(q-l)
3 Find e relatively prime to Ø, i.e. gcd(ø,e)=1; 1<e<ø. {e,n} is R's Public Key
4 Find a number d which satisfies relation
(d * e) mod (ø) =1
{d,n} is R's Private key
5. Let plain text = t. Encrypt t using R's public key.
Encryption = t^{e} (mod n) = c (cipher text)
6.Decryption c^{d} (mod n) =t
(Both n and e should be known to encrypt. Similarly both n and d should be known to decrypt)

Example Of RSA Use

This example is a toy example to illustrate the method. In practice the primes p and q will be very large – each at least 300 digits long to ensure security.

RSA Algorithm

1.Pick as prime numbers p=3,q=11
n = p * q=33
Note : The message to be encrypted should be smaller than 33.If we do letter by letter encryption of English alphabets (A to Z as 1 to 26) this is OK
2. Ø = (p-1) x (q-1) = 2 x 10 = 20
3.Pick a number relatively prime to 20.
We pick 7. The Public key of R = {7,33}
4.To pick private key of R find d from relation (d x e)mod(ø) =
1 (d x 7) mod (20) =1
This gives d =3
Therefore, the private key of R = {3,33}

Applying RSA Algorithm

1.Let the message be CODE

If we use code C=3, O=14,D=4,E=5

The message is 3,14,4,5

2.We will encrypt one letter at a time

Thus cipher of plain text 3 is

3^{e} mod (n) $=3^{7}$ mod(33)

3^{7} mod (33) =2187 mod (33)=9

$(14)^{7}$ mod (33) = 105413504mod(33)=20

$(4)^{7}$ mod (33) =16384 mod (33) =16

$(5)^{7}$ mod (33) =78125 mod(33) = 14

3.Thus cipher text = 9,20,16,14

4. Decryption : c^{d} mod (n) d=3,n=33

9^{3} mod (33) = 729 mod(33) = 3

20^{3} mod(33) = 8000 mod(33)=14

16^{3} mod(33) = 4096 mod(33) =4

14^{3} mod(33) = 2744 mod(33) =5

We see that we get the original text 3,14,4,5

Discussion on RSA

• The security RSA encryption is dependent on the fact that factorising a large prime number to its factors is very difficult.

• RSA algorithm is symmetric. In other words if a plain text is encoded by the private key of S, the sender, it can be decrypted using the public key of R, the receiver (We will find later that this symmetry property is used in creating digital signature)

•Example using S's keys

S's Private key = {3,33}
S's Public key = {7,33}

• If we encrypt a plain text using S's private key and send it to R,R must be able to decrypt it with S's public key.

•Assume Plain text is encrypted with S's private key and get cipher text = $(14)^{3}$ mod (33)=5

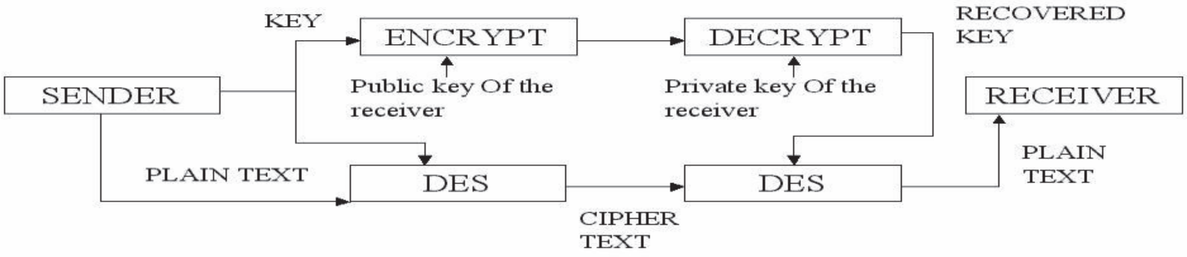
•Decrypting with S's Public key we get

$(5)^{7}$ mod (33)
=78125 mod(33)
={(2367 x 33) + 14} mod (33)
=14

DISCUSSION – RSA Vs DES

•RSA Public key has two keys – a private secret key and a public open key.
•RSA implemented as a program (software) It is computationally complex to encode plain text and decode cipher text using RSA
•DES Same key for encryption and decryption. It is a single key system - Also called symmetric key system
•DES computationally simple-implemented in hardware - thus very fast •Each communication between two businesses can use a different key – provided key is securely exchanged
•If key can be sent separately encrypted using RSA, then a recipient can use this to decrypt DES encrypted message.

Combining RSA And DES



Advantages:

- Key is sent along with the plain text. Encrypted using RSA
- Key is small-fast to encrypt/decrypt
- Each transaction using DES can have a different key- higher security and also fast.Key directory not needed.

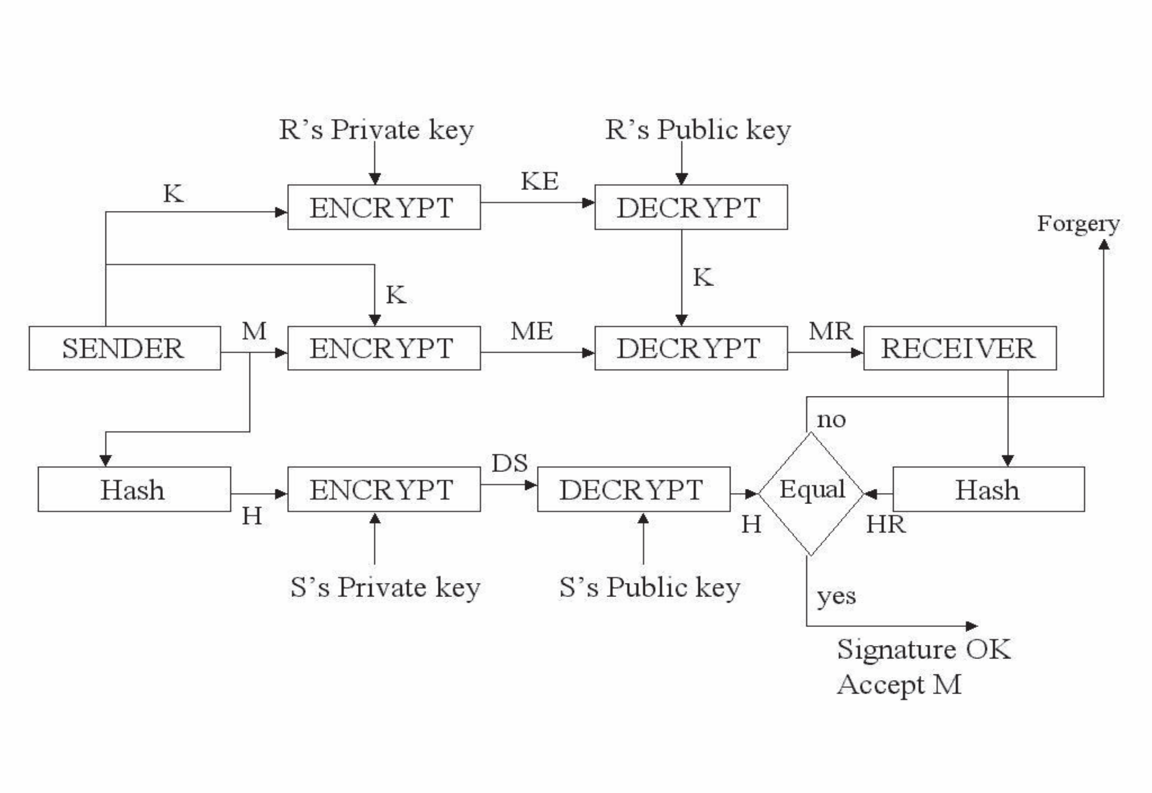
Digital Signature

REQUIREMENTS

•Needed to ensure that a message received from say "A" is indeed from him
•Signature should be tied to the message sent by "A"
SENDING STEP
•Sender sends key using RSA system
•Sender sends plain text "M" using DES
•Receiver decrypts cipher text using DES and the key received from sender call it "MR"
•Sender hashes plain text "M' using a hashing function - let the hashed text be "H"
•Hashed text "H" encrypted by sender using his Private key
•DS is his signature as H encrypted with his private key
•DS decrypted by receiver using sender's Public key and obtains "H"

Authentication step
•Receiver hashes “MR" using hash function and gets “HR"
•Receiver compares “H" with “HR"
•If they match then it is a signed authenticated plain text
•TM is signed as sender has encrypted the hashed text using his private key which he only knows.If H=(MR)(HASHED) = HR where MR is the received message then MR must have been sent by sender. He cannot repudiate.

Signing A Message Using Digital Signature



Certificate Authority For Digital Signature

•As the hashed message in Digital Signature system is decrypted using senders public key, this key must be certified as belonging to sender by an independent authority

•Certification needed to ensure authenticity of public keys of organizations as public key is used to verify signature

•Certification authority keeps data base of public keys of organizations participating in e-commerce after verifying their credentials.

•Potential business partners can authenticate public keys by sending request to certifying authority who certifies after receiving a fee for his services