

Network Security

Ch 8

RJ Department of Computer Science 2008

Cryptography

g Services Provided

- Confidentiality
 - Protection of data from eavesdroppers
- Authentication
 - I am exchanging information with whom I believe I am exchanging information with
- Integrity
 - I received what was sent without replays, modifications, insertions or shuffling

RJ Department of Computer Science 2008

Components

- g Algorithm & Key are two main components
- g Algorithm that depends on its secrecy is vulnerable
 - Disassembly & reverse engineering possible
- g System depends on Keys
 - Set lifetime
 - evade cryptanalysis
 - Minimise damage due to compromised key

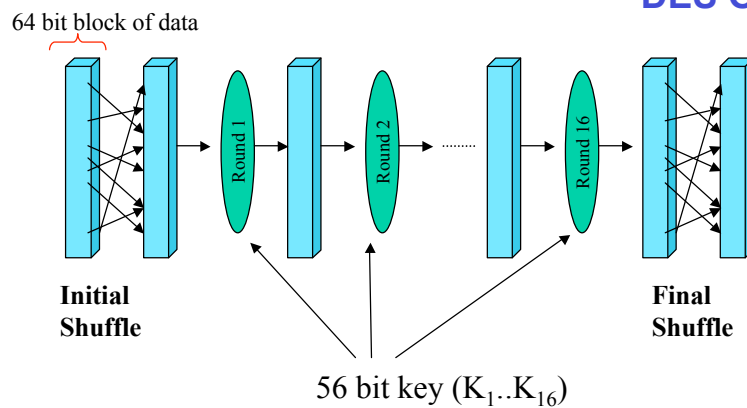
Cryptographic Algorithms

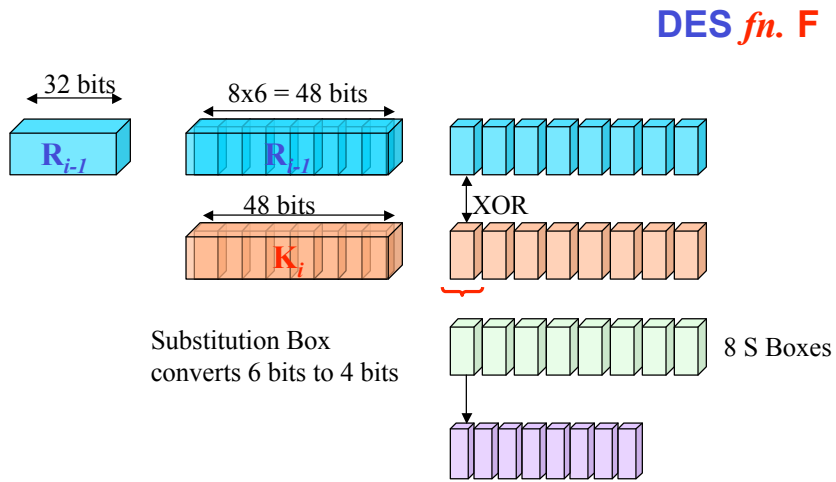
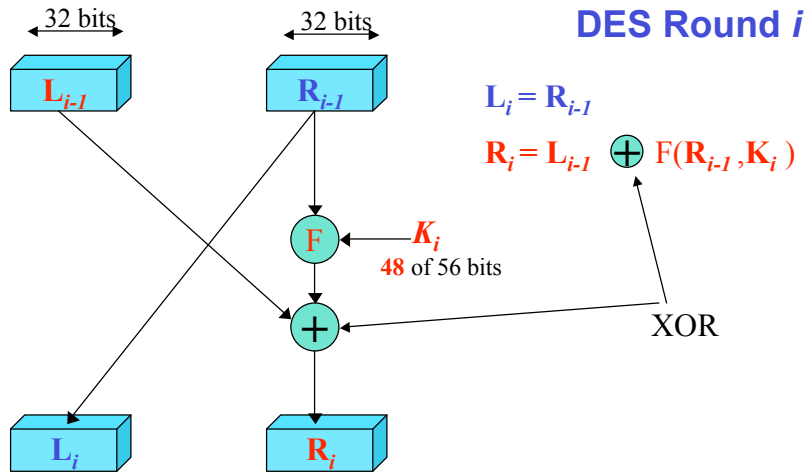
- g Secret Key Algorithms
 - Data Encryption Standard (DES)
 - Intl' Data Encryption Algorithm (IDEA)
- g Public Key Algorithms
 - Rivest, Shamir, Adleman (RSA)
- g Hashing Algorithms
 - Message Digest 5 (MD 5)
- g Cryptographer Vs Cryptoanalyst

Good Keys

- g Avoid many repeating characters/patterns
- g Avoid visible patterns (human eye recognizable)
- g Secure storage
- g Longer the better
 - Theory : Any cryptographic system can be broken by brute force

DES Outline





Cipher Block Chaining (CBC)

- g Large messages are split into 64bit blocks
- g Ciphertext for $block_i$ is XORed with plaintext for $block_{i+1}$
- g Initialization Vector (IV) is used as ciphertext for $block_0$
 - A Random number sent by sender.
- g Confusion & Diffusion provides security

RSA

- g Public Key Encryption
- g Private Key for Decryption
- g Algorithm is public knowledge

- g Fact: It is easy to multiply 2 large prime numbers, but computationally difficult to find the factors of their product

RSA: Pub. Key & Pvt. Key Generation

p, q : Prime numbers ~256 bits long

e : encryption key
 e & (p-1) x (q-1) are relatively prime
 [1 is the GCD of these two numbers]

$$n = p \times q$$

$$d \cdot e \pmod{\{(p-1) \times (q-1)\}} = 1$$

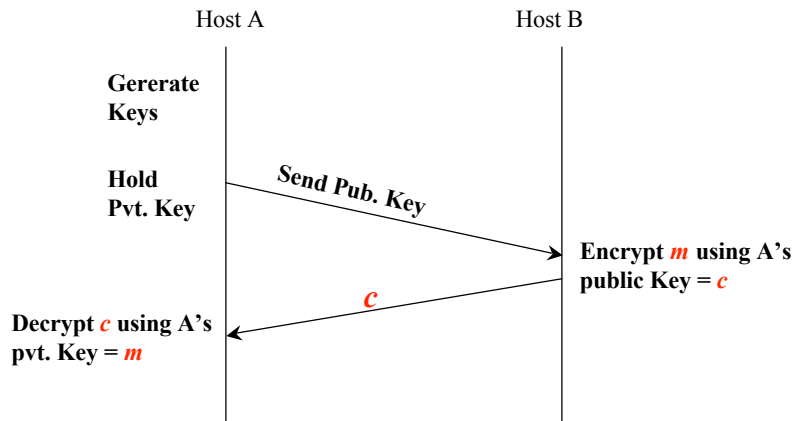
Public Key : <e,n>

Private Key: <d,n>

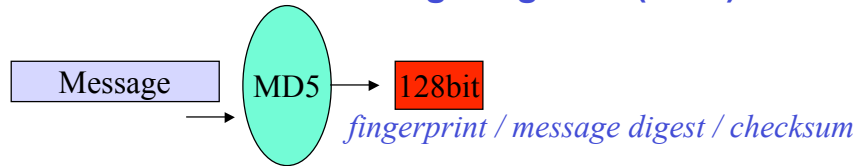
Discard p & q

Encryption : $c = m^e \pmod n$
 Decryption : $m = c^d \pmod n$

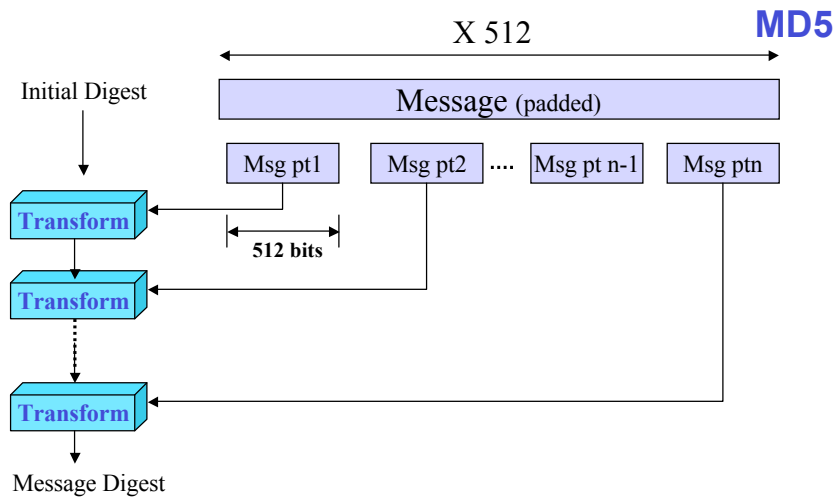
Privacy



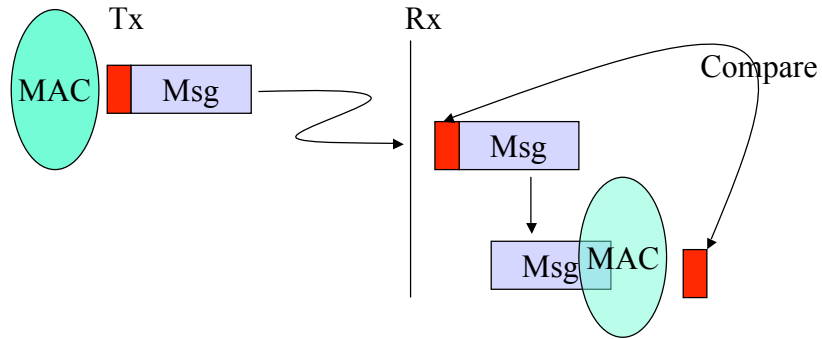
Message Digest 5 (MD5) RFC 1321



- ❖ Computationally infeasible to produce:
 - 2 messages that results in same digest
 - Message that will result in a pre-specified digest



Message Authentication Code (MAC)



Speed

Encrypt	Software	VLSI
MD5	600 Mbps	Gbps
DES	100 Mbps	Gbps
RSA	100 Kbps	Kbps

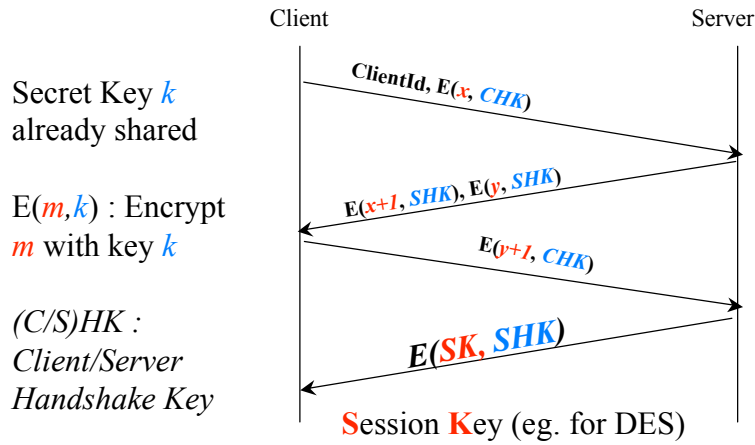
Archival Security

- g 3DES
 - DES is borderline secure
 - 2 or 3 keys used for triple DES
- g RSA : 1024 bit or 2048 bit keys

Security Mechanisms

- g Authentication Protocols
- g Message Integrity Protocols
- g Public Key Distribution

Auth: 3way Handshake



Secret Key k
already shared

$E(m, k)$: Encrypt
 m with key k

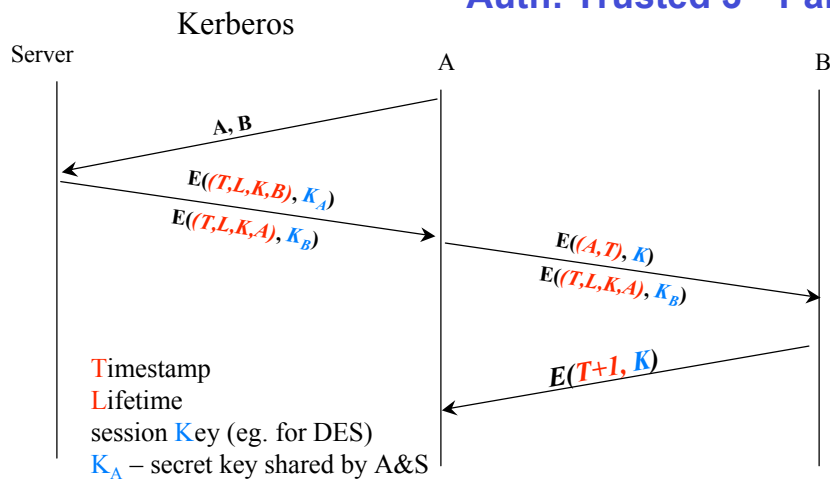
$(C/S)HK$:
Client/Server
Handshake Key

RJ

Department of Computer Science

2008

Auth: Trusted 3rd Party

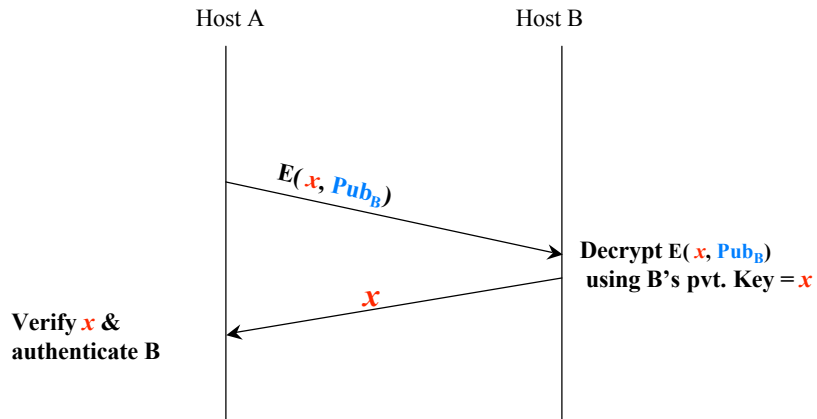


RJ

Department of Computer Science

2008

Auth: Public Key



Integrity: Digital Signature w. RSA

- g System to assure $E(m, k)$ and thus m was generated by only one participant
- g Sender uses Pvt. Key, receiver uses sender's public key to decrypt $E(m, k)$.
- g Reverse property of RSA relative to privacy.

Integrity: Keyed MD5

- g MD5 has no secret key.
 - authenticity issue: Imposter can send msg with MD5 checksum.
 - integrity issue: Imposter can intercept & alter msgs.

Tx & Rx share secret key k

Tx sends : $m + \text{MD5}(m+k)$

Integrity: Keyed MD5 with RSA

- g What if there is no shared secret Key

Tx sends : $m + \text{MD5}(m+k) + E(k, R_{X_{\text{PUB}}})$

What's wrong above?

Tx sends : $m + \text{MD5}(m+k) + E(E(k, R_{X_{\text{PUB}}}), T_{X_{\text{PVT}}})$

- g How does Rx get $T_{X_{\text{PUB}}}$?

Integrity: MD5 with RSA signature

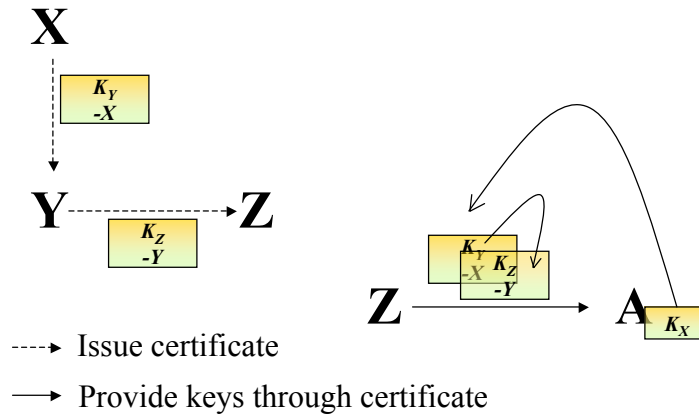
- g Tx: sign MD5(m) with Tx_{PVT}
- g Tx sends: $m + E(\text{MD5}(m), Tx_{PVT})$
- g @ Rx
 - Run MD5 on m
 - Use Tx_{PUB} to decrypt $E(\text{MD5}(m), Tx_{PVT})$
 - Compare checksums

Public Key Distribution

- g How does A convey its $K_{A.PUB}$ to B?
 - Earlier mechanisms assume public keys came from authentic sources
- g Digital Certificates
 - Binding 'identity' with 'public key'

I certify that the following key belongs to A
 $K_{A.PUB}$
-signed(Certifying Authority)

Chains of Trust



Tree-structured CA Hierarchy

- g Everyone has public key of root CA
- g A → B chain of certificates sufficient to build chain of trust
 - What if some CA issues certificates recklessly?
 - Arbitrary Mesh for chain of trust (eg.PGP)

X.509 Standard

- g Components of certificate
 - Name of entity being certified
 - Public key of entity
 - Name of CA
 - Digital Signature
 - Algorithm used

- g Certificate Revocation
 - Certificate revocation List

RJ Department of Computer Science 2008

Pretty Good Privacy (PGP)

- g E-mail tool
- g PGP stores certificates in a *'key ring'*
 - Relationship b/w certificates forms arbitrary mesh
 - Levels of trust assigned to each certificate based on the relationship in mesh (who issued certificate to who)
 - # certificates for an entity also counts towards trust
- g Encryption
 - Tx sends : $DES(m + k) + E(k, R_{x_{PUB}})$
 - K generated per message
- g Integrity & Authentication
 - Tx sends : $m + E(MD5(m), T_{x_{PVT}})$

RJ Department of Computer Science 2008

Secure Shell for Remote Login(SSH)

- g telnet & rlogin
 - Login details sent in clear
- g Step1 : setup transmission channel SSH-TRANS b/w client & server
 - Client authenticate server using RSA
 - Client has to have server's public key
 - First time key distribution
 - Establish session key
 - Eg. For 3DES

SSH

- g Step 2 : Authenticate client
 - Password
 - Public key encryption
 - Client's public key has been already placed in server
 - Host-based authentication
- g Extensions
 - SSH tunnel for TCP apps (eg: IMAP mail & X-Windows)

Transport Layer Security (TLS, SSL, HTTPS)

- g General purpose secure sub-layer protocol
 - b/w Appl. & TCP layers
 - TCP provides its normal features (flow control, congestion control, reliability etc..)
 - Appl. Provided TCP ports (eg. HTTPS : 443)
 - RT negotiation of encryption algorithms
- g Handshake – to set up shared state secure communication
- g Record – actual data transfer

IPSEC

- g Framework to provide security services
 - Mandatory in IPv6
- g Authentication Header (AH)
 - Access control, connectionless message integrity, authentication, antireplay protection
- g Encapsulating Security Payload (ESP)
 - All of above + confidentiality
- g Internet Security Association & Key Management Protocol (ISAKMP)

Security Association

- g SA is one-way connection
 - binds ISAKMP & {AH, ESP}
- g Each SA is assigned a Security Parameters Index (SPI) by RX host
- g SPI-Rx IP address pair identifies an association
- g ISAKMP – defines procedures and formats to manage SA.