Authentication

RSA – Rivest Shamir Adelman

Encryption of plaintext m: $c = m^e \bmod n$

Decryption of cyphertext c: $m = c^d \bmod n$

Note that

$Pbl_A(Prv_A(m)) = m$ & $Prv_A(Pbl_A(m)) = m$

Encrypted message, readable only by A	$Pbl_A(m)$
Signed message of A, readable by all	$Prv_A(m)$
Signed message of A, readable only by B	$Pbl_B(Prv_A(m))$

but the public key is expensive
and how will the receiver obtain the public key

Message Digests and Secure Hashes

Transform long text sequences into short signatures

MD5 – RFC 1321, Ron Rivest

`openssl dgst -md5` on Linux

A cheaper signed message

$m + Prv_A(MD5(m))$

A cheaper signed and encoded message (one of many methods)

Choose session key K

Send $Pbl_B(Prv_A(K))$

Send $DES_K(M)$

Authentication methods

Public Key – discussed above

Challenge / response

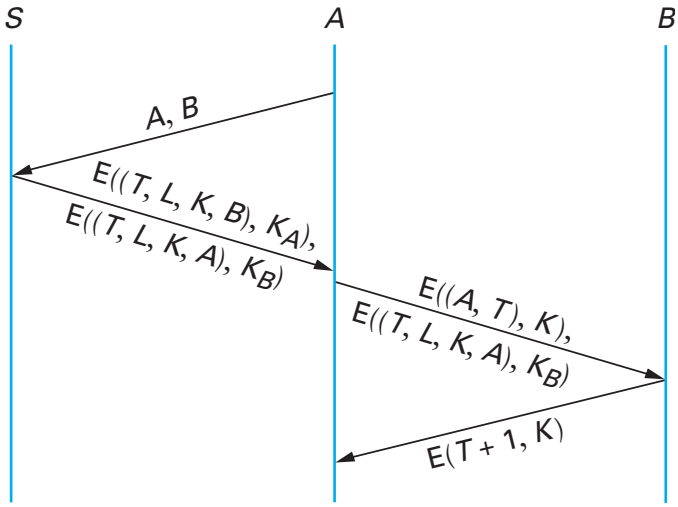
Client authenticating self to server

Server → Client: Random number (nonce)

Client → Server: *E*(nonce)

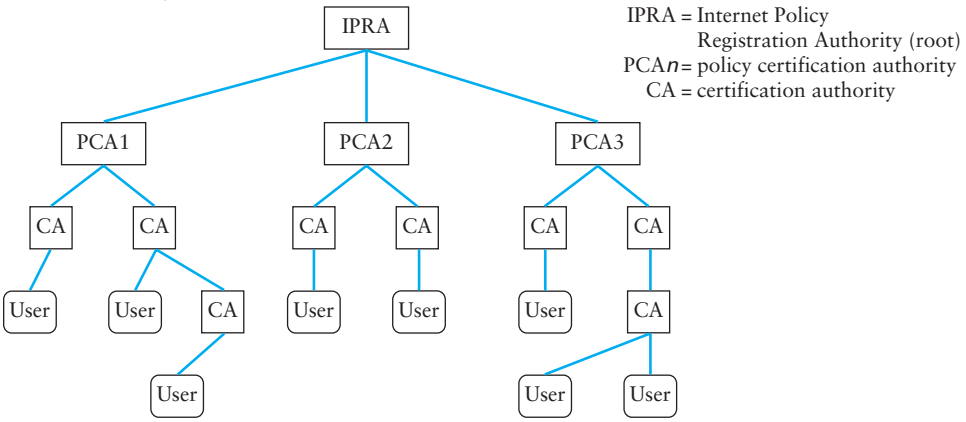
Microsoft NTLN challenge / response

Kerberos (MIT, Windows 2000 active directory)



A: Client
B: Server
S: Trusted third party
K_A: Key shared by A and S
K_B: Key shared by B and S
T: Timestamp
L: Lifetime for timestamp
K: "Session" key
E(m,k): Message m encrypted with key k

Public Key Infrastructure – PKI (X.509)



Certificates in Java
Certificate Authority Services