SYMMETRIC KEY CRYPTOGRAPHY

- AES
- Blowfish, Twofish
- Skipjack
- IDEA
- DES + 3DES

Symmetric Algorithms

Block cipher

- 640 bits of message chopped into → 10 individuals block of 64-bits
- Strong cipher contains two attributes
  - Confusion – Substitution
  - Diffusion – Transposition
    - Related concept "Avalanche Effect"
    - A tiny input to Algorithm significantly change the output

Stream cipher

- Individual bits of plaintext XORed to produce ciphertext
- Uses Keystream Generators

STREAM CIPHER

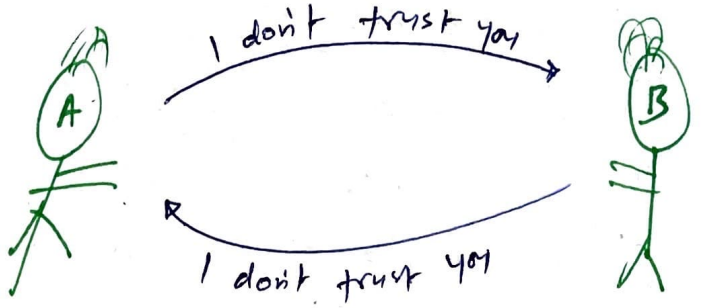
- Requires randomness (refer to IV concept)
- Require more processing power, so used at hardware level while Block cipher takes less processing power & suited at software level.

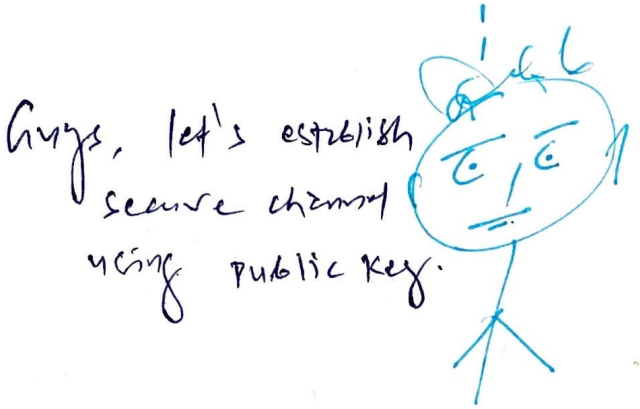
Symmetric Key Cryptography

e.g.

- Secret key Cryptography
- Session key Cryptography
- Shared key Cryptography
- Private key Cryptography

7. PKI & CRYPTOGRAPHIC APPLICATIONS





PERSPECTIVE

Asymmetric Cryptography

Networking

Email

Web

Digital Right Management

E-commerce

Applications

Attacks

World of PKI

Certificates

ASYMMETRIC CRYPTOGRAPHY

Three most common public key cryptography system used today:

1. Public & Private Keys
   - Public key freely available to anyone with whom they want to communicate.
     (BATMAN VS JOKER)
   - Beauty of public key cryptography

2. RSA
   - 1024 bits KL
   - has one-way function
   - Factors large prime numbers into their original prime numbers.

   jump:- RSA often used as key exchange protocol, means it can encrypt symmetric key for secure delivery to destination.
   (RSA often used with AES)

ELGAMALDOUBLE

El Gamal

Plaintext 2048-bits → Encryption → ciphertext 4096-bits

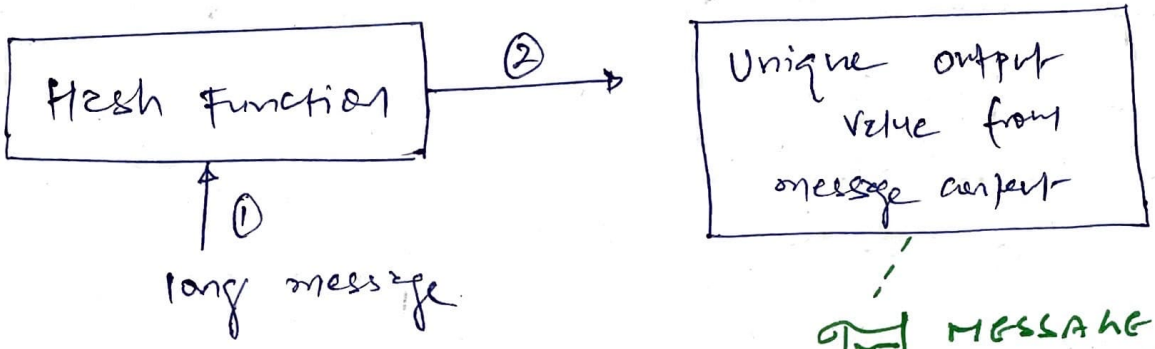
- it doubles the length of message it encrypts, data transmission becomes hard for narrow bandwidth circuits.

CRYPTOSYSTEM	KL
RSA	1024 bits
DSA	1024 bits
Elliptic curve	160 bits

- Equivalent

Any input
Fixed output → # HASH FUNCTIONS ... ONE-WAY
... collision-free

cryptography system	&	Digital signature	→	Integrity



MESSAGE DIGEST (MD) 128-bit or larger

MD Generated by Sender & transmit to receiver with message for two versions.

Receipient can use same hash Function to recompute MD.
If values same = good.
If values are diffrent = message was tempered.

MD can be used to implement Digital Signature

INTEGRITY

NON REPUDIATION

* Four common hashing Algorithms :

SHA

- Secure Hash Algorithm

SHA-1

- takes an input of arbitrary any length & Produces 160-bit message digest.
- Process message in 512-bit blocks

SHA-2 : Four variants

a) SHA-256
- 256-bit MD
- 512-bit block size

b) SHA-224
- truncated version of SHA-256
- 224-bit MD
- 512-bit blocksize

c) SHA-512
- 512-bit MD
- 1024-bit blocksize

d) SHA-384
- 384-bit MD
- 1024-bit blocksize

HAVAL

- Hash of variable length
- Produce MD of 128, 160, 192, 224 & 256 bits

MD2

- 128-bit MD

MD4

- 128-bit MD
- 512-bit blocksize

MD5

- 128-bit
- HAVAL is MD5 variant

MD2 + MD4 + MD5 + SHA-1

NOT SECURE

SHA-2

Almost secure but has SHA-1 weaknesses.

SHA-3 SHA-384

∴ Federal Govt. approved Digital signature standard

DIGITAL SIGNATURES

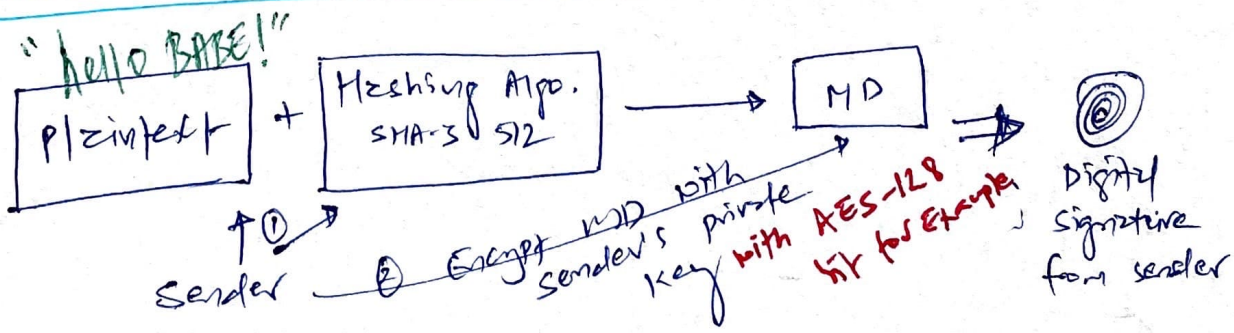
one of the reason why message digest (MD) is created. To implement Digital signatures.

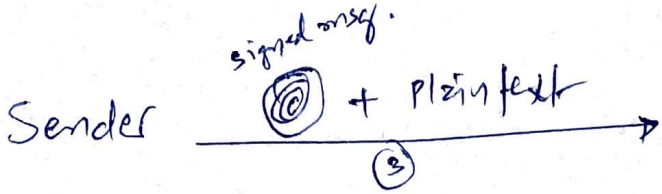
2 Goals

- To enforce Non-repudiation
- To maintain Integrity of the message

Digital signature Algorithm = 1. Public key Cryptography + 2. Hashing Functions

Process (Refer to remarkable notes)





④ Decrypt msg with sender's public key

Receiver also creates MD with same hashing function & plaintext ⑤

⑥ Receiver compare his MD with sender's MD — Match! / Don't match.

digital signature → yes
Integrity, Authentication, Nonrepudiation

↓ NO
Confidentiality

Trivia :- What can sender do / add extra step for message privacy / confidentiality ?

Ans: We can encrypt entire Digital Sig. process with Asymmetric Encryption

Need Partial Digital Signature ?

→ HMAC
(Hashed message authentication code)

Relies on shared secret key

⇓

Symmetric key cryptography

✓ Integrity

✗ Nonrepudiation

Digital Signature Standard (DSS)

→ Acceptable for Federal Information processing Standard (FIPS) 186-4

→ Must use SHA-3 Hashing Function

3 Approved standard Encryption Algorithms

→ Digital signature Algorithm (DSA) --- FIPS 186-4

→ RSA Algorithm ------ ANSI X9.31

→ Elliptic-curve DSA (ECDSA) --- ANSI X9.62

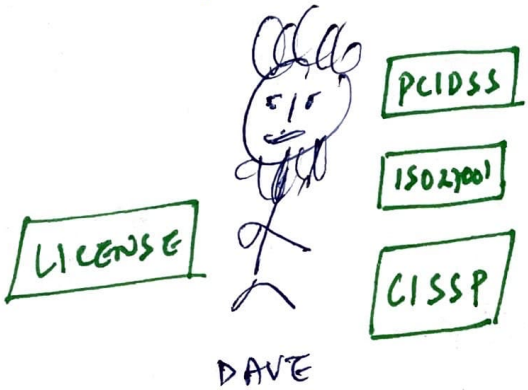
PUBLIC KEY INFRASTRUCTURE (PKI)

Nonrepudiation, Integrity, Authentication & Confidentiality: provides

PKI = पंजीयन

To establish communication b/w two parties that are previously unknown to each other.

* certificates = Endorsed copy of Individual



All of these certificates are signed by respected certificate Authority (CA)

(ISC)²

VICRoads

GoDaddy

Digicert

They validate user identities & give heads-up to CAs to issue Digital certificates.

Registration Authorities

Assist

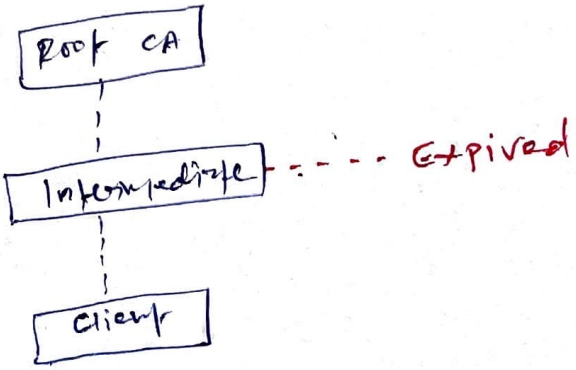
Certificate Authorities

vistaIndia

offload Burden

Netflix

Certificate Path Validation (CPV)



* Certificate Generation & Destruction

nothing but a Public Key

Enrollment

① Prove your identity to CA / VicRoad

② Provide your public key to CA

③ CA creates X.509 digital certificate that contains your identity + public key

④ CA signs (digitally) with CA's private key certificate

⑤ We can safely distribute with other parties / drive on the road.

we can decrypt with our public key (or) this could be CA's public key

Verification

* When we receive digital certificate from someone with whom we want to communicate

↳ check CA's digital signature using CA's public key

↳ check if certificate is revoked (CRL)

↳ OCSP

② Either we can provide our public key to CA or we can ask CA to provide public key + private key

Revocation

Certificate Revocation List (CRL)

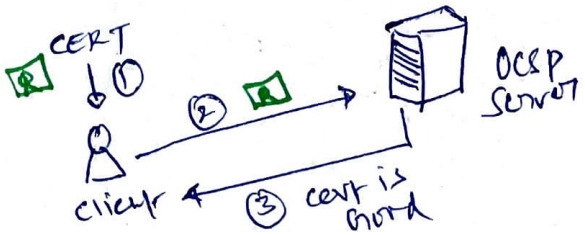
- Part of CA's inventory
- Most common method but huge latency.

Note - CRL contains serial number of Digital certificates, serial number must be part of CRL

CA must provide private key to requested party in most secure manner

Online Certificate Status Protocol (OCSP)

- Removes CRL's latency
- Real-time verification



ASYMMETRIC KEY MANAGEMENT

- Consider Key length
- Secure key in Vault
- Key Rotation
- Backup Key
- Retire Key after use
- Use Key Escrow Service

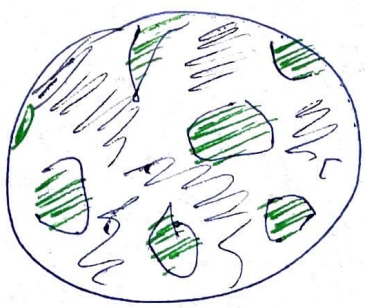
HSM — Hardware security modules

- Hardware devices to store & manage encryption keys

Cloud-based HSMs

YUBIKEY

APPLY CRYPTOGRAPHY



REAL WORLD APPLICATIONS

APPLIED CRYPTOGRAPHY

Data at rest

Portable devices

- Most OS = Encryption file system + smartphones
- Modern computers =
  - TPM (Trusted platform modules)
    - Storage & mgmt of keys used for Full Disk Encryption (FDE) solutions.

Data in transit

Email

If you want

- confidentiality → Encrypt the msg
- Integrity → Hash the message
- Authentication + Integrity + Non-repudiation + Confidentiality → Encrypt the msg + digital signature

Secure Email

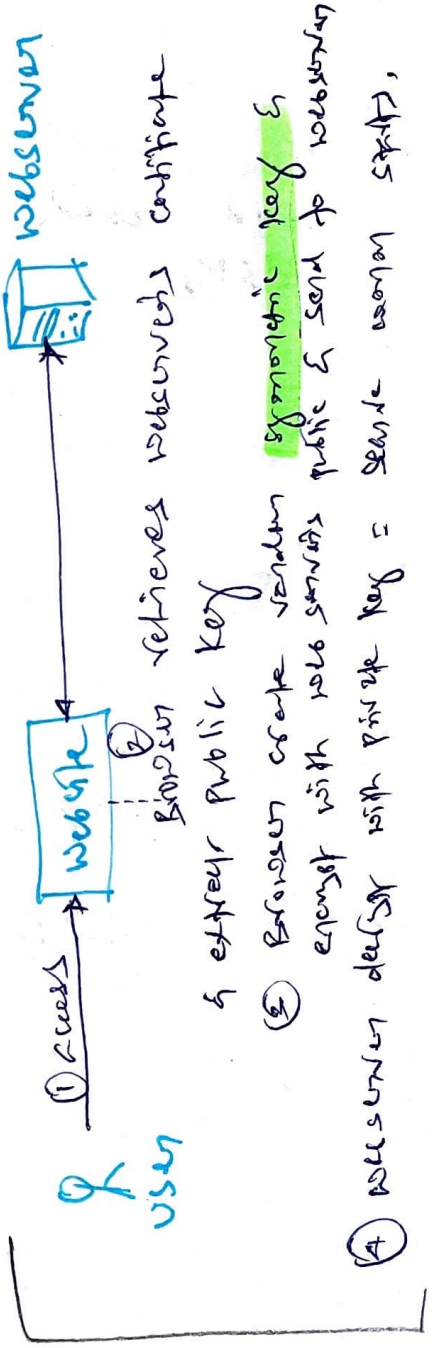
- P.T.O End → PGP
- S/MIME (use of X.509)

Steganography & watermarking

Risky ...

Web Application

- SSL 3.0 → Poodle vulnerability
- TLS V1.2 ... Heartbleed



why this approach is facilitating Up to End

DRM s/w uses ENCRYPTION to enforce copyright restriction on digital media.

DRM - Digital Rights Mgmt

music

movies

ebook

Video Game

Document

High Bandwidth Digital Content protection (HDCP)

- HDMI, DVI interface, display port

Adobe provides ADEPT - Adobe Digital Experience Protection Technology

Uses AES for encryption & RSA for encryption to protect AES key.

Use encryption to protect docs/ sensitive info.

Advanced Access Content System (AACS)

- Blue-ray, DVD media

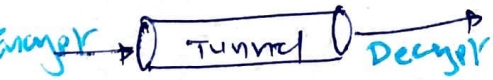
Networking

CIRCUIT ENCRYPTION

2 Encryption techniques to protect data while traveling over networks

Link Encryption

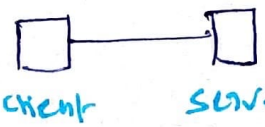
- Protects entire circuit



IPSec

End-to-End Encryption

- Protects comms b/w two parties



TLS 1.2
SSH

Wireless Security

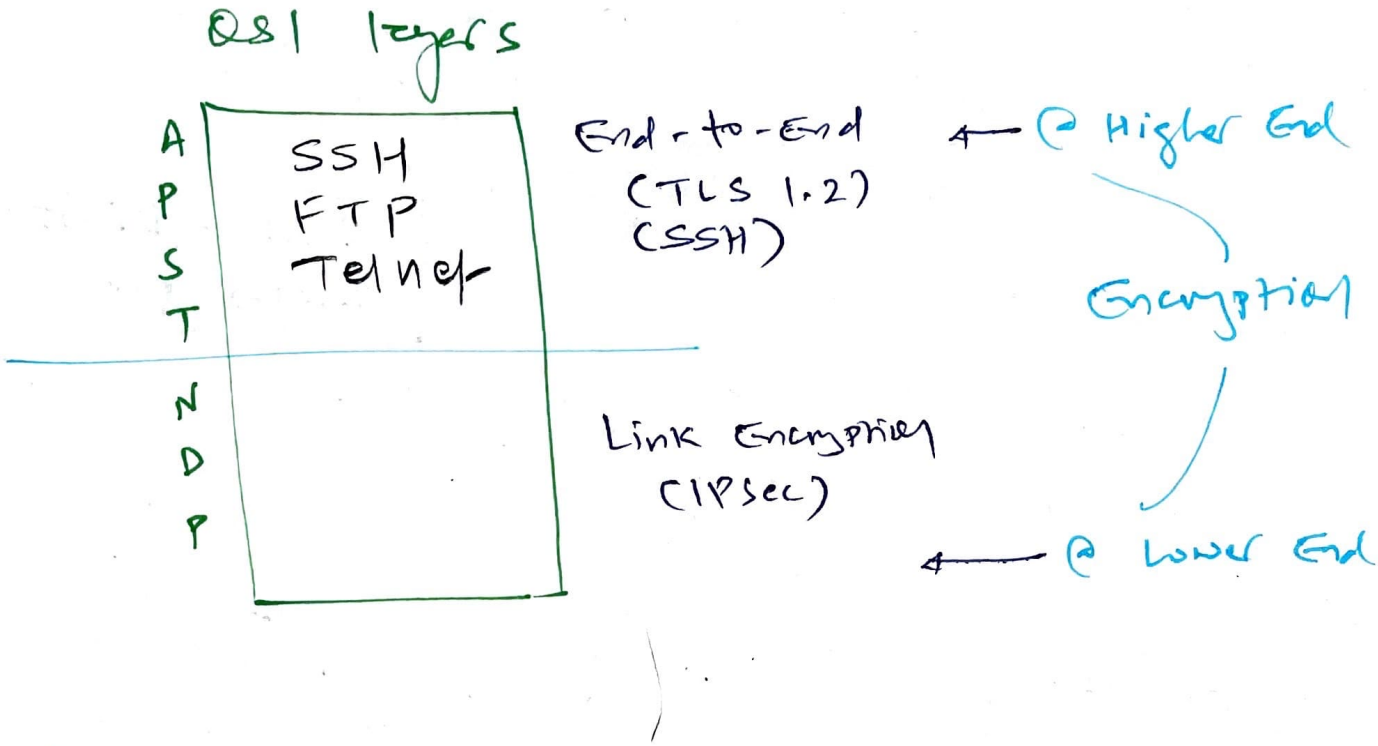
WEP

- 64 & 128-bit encryption
- Not secure

WPA

- Eliminates weakness of WEP with TKIP

WPA2 uses Temporal Key Integrity Protocol AES cryptography



* IPSec

- Uses public key cryptography
- Provides Encryption, access control, non-repudiation & message authentication using IP Protocols.
- Prime use : VPN
- 2 operations

Transport mode (P2P)
- only packet payload is encrypted. Good for P2P.

Tunnel mode
- Entire packet + header is encrypted
- Ideal for gateway to gateway comms.

- IPSec relies on Security Associations (SA)

AH
- Authentication Header
- Provides message integrity, non repudiation, access control to prevent replay attacks.

ESP
- Encapsulating Security Payload
- provides confidentiality & integrity of message
- Limited encryption & Authentication to prevent replay attacks.

IPSec runtime

↳ Creates SA

- To represent communication session
- Record configuration about session

Requires 2 SA for bi-directional

ISAKMP (manages SA)

- Internet Security Association & Key mgt protocol
- ISAKMP: provide background support for IPSec
  - ↳ Negotiate, establish, modify & delete SAs

4 requirements.

1. Authenticate communicating peers
2. create + manage SAs
3. Provide key generation mechanisms
4. Protect against threats: DDoS, Replay.

CRYPTOGRAPHIC ATTACKS

↳ Analytic Attack

↳ side channel Attack (Timing Attack)
- Stalk her to find out where she work, what she does for living.

↳ Implementation Attack - Exploits (implementation flaws)
↳ e.g Heartbleed Bug + Reverse Engr.
↳ SCA (Source code Analysis), most common method to find

↳ Statistical Attack (Frequency Analysis Attack)
- identifies the pattern

↳* Brute force
- Randomly find correct cryptographic keys
- KL is important

Enhanced Attack : Rainbow Table

Use cryptographic SALT

Password	Random number

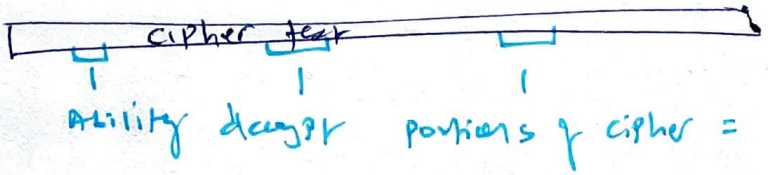
↳ ~~Frequency Analysis~~ Ciphertext only Attack

Attacker has ciphertext & their goal is to find key used in Encryption process

↳ * Known plaintext : Attacker has copy of

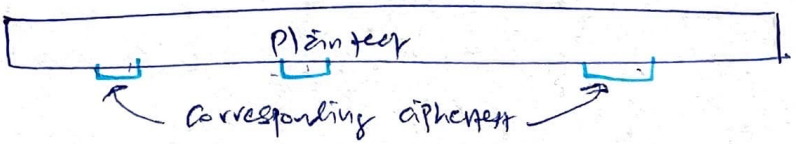
(ciphertext)
Encrypted + plaintext message → To know the key how cipher text generated from

↳ chosen ciphertext



Attacker : Ability decrypt portions of cipher = to know key

↳ chosen plaintext



Attacker : Ability to extract plaintext portion to determine which encrypted algorithm is used.

↳ Man in the middle
↳ 2DES is vulnerable of this.

↳ * MitM (man in the middle) — Attacker establish secure connection to client & all comms to legitimate server goes via his machine.

prevention:

↳ Birthday
A.K.A — collision or Reverse Hash matching
— To find if different msg produce same message digest

↳ * Replay → malicious user intercepts encrypted message b/w two parties & Replay the captured message to open new session.

pass the Hash p.t.o end

Prevent using expiration of msg or incorporate timestamp.

To Secure Email

PGP

- Pretty Good privacy
- Combines CA hierarchy with "Web of trust" concept
  - you have to (must) become trusted by one or more PGP users to begin using the system.

* 2 versions of PGP

Commercial

- Use RSA for key exchange
- IDEA for Encryption/Decryption
- MD5 for digest production

Freeware

- Use DH for key exchange
- Use CAST 128-bit Encryption/Decryption
- Use SHA-1 hashing function

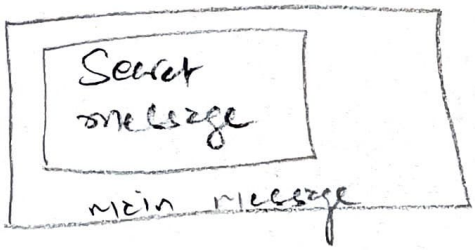
S/MIME

- Secure/Multipurpose Internet Mail Extension
- Uses RSA Encryption Algorithm
  - O365
  - Lotus
  - Mac OS X mail
  - Mozilla Thunderbird
- Relies on X.509 for exchanging cryptographic keys
- RSA is only Public key cryptographic protocol supported by S/MIME

most facinating approach

- Web Browsers & web servers use private/public key with Asymmetric cryptographic approach but web browser uses Symmetric keys for speed.
  - this is awesome (OSI P 257)

Steganography



Art of using cryptographic technique to embed secret message within another message.

Brute-force Attack

- Use salt
- longer key length
- Key stretching

Work factor — if any of below 3 element is work, attacker can break the cryptosystem

1. Algorithm without flaws
2. Large key size
3. protect the secret key

Pass the Hash – Replay Attack

Targets AD.

Countermeasures

- Timestamps
- Sequence Numbers