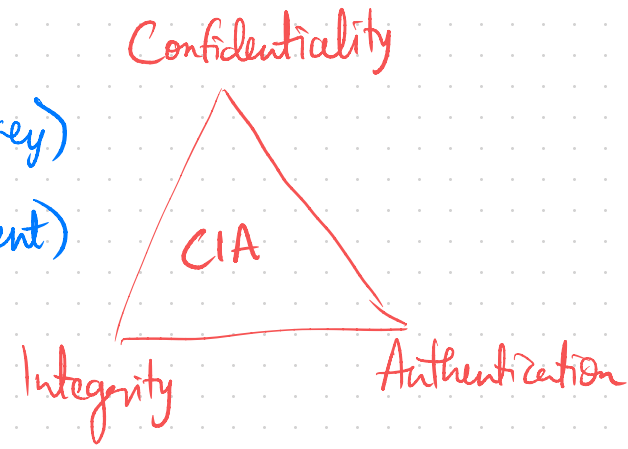
chapter 20

Cryptography

Concepts

- Symmetric (same key)
- Assymmetric (different)



GAK

- Government Access to Keys
- Copies of some keys to government
- Government uses when court issues warrant
- Similar: wiretapping.

Algorithms

DES, AES, RC4, RC5, RC6

DSA, RSA, MD5, SHA

Cipher

Types of cipher

- classic cipher
  1. Substitution (replace)
  2. Transposition (shift)
- Modern cipher
  - Based on Key
    1. Private key (same)
    2. Public key (different)
  - Based on Input Data
    1. Block (fixed)
    2. Stream (continuous)

DES

- 64 bits data; 56 bit key
- archetypal block cipher
- inherent weakness — cracked
- 3DES added strength.

AES

- Symmetric
- iterated block cipher.
- 128 bit data; 192, 256 bit keys

RC4 – Symmetric; random permutation (byte)

RC5 – Parameterised algorithm; variable characteristic (block, key, rounds)

RC6. – Symmetric; 4 bit register; integer multiply.

Blowfish - replacement of DES / IDEA

Twofish

- 128 bit data ; 256 bit key.
- flexible with network based apps.
- enables memory, hardware, encryption Performance.

Threefish

- tweakable symmetric key
- 256, 512, 1024 bit key
- 3 operation: Addition - Rotation - XOR
- 256, 512, 1024 data

Serpent

- 128, 192, 256 bit block data.
- 32 operating rounds (Substitution, Permutation)

TEA

- Tiny Encryption Algorithm; Feistel cipher.
- 128 bit key; 64 bit block data.
- Uses constant: 232 - golden ratio.

CAST-128

- symmetric key block cipher
- 12/16 round feistel network
- 40-128 bit key (8-increments)
- used in GPG, PGP.

GOST (Magma)

- Symmetric block cipher.
- 32 round feistel network
- 64 bit data ; 256 bit key
- S-box → secret, 354 bit secret.

Camellia

- Symmetric key block cipher
- 18-24 rounds (128-256 bit)
- 128 bit data ; 128, 192, 256 bit key.
- used in TLS protocol.

Digital Signature

- generation & Verification of DS
- set of rules, parameter

RSA

- Public key cryptosystem
- Internet encryption, authentication.
- Modular arithmetic, Number theory.

Diffie-Hellman

- establish shared key - Insecure channel
- No authentication for key exchange.
- vulnerable to many attacks.

YAK

- Public key based key exchange Protocol
- Authentication: Public key Pairs.
- Uses PKI → distribute public keys.
- Variant of two pass HMQV.

Hashes – MD5, MD6

- MD5 → 128 bit fingerprint.
- No collision resistant
- MD6 → Merkle tree structure.
  → Parallel computation
- Used for integrity check, storing Passwords.
- MD6, SHA2, SHA3 → recommended.

SHA

- Secure one way hash.
- SHA 1 → 160 bit digest. ~ MD5
- SHA 2 → 256, 512 bit
- SHA 3 → Sponge construction

RIPEMD-160

- RACE Integrity Primitive Evaluation Message Digest
- 160 bit hash
- also 128, 256, 320 available.
- 80 stages (5 blocks)
- modulo 32 addition — twice.

HMAC

- type of Message Auth code.
- Crypto key + Crypto Hash. (SHA, MD5)
- protects from length extension attack.

Elliptic Curve

- Public key Cryptography
- avoid larger key usage.
- number theory, math elliptic curve.
- replacement of RSA.

Quantum

- Quantum Mechanics; key distribution.
- encrypted: Sequence of photons

Homomorphic

- Process encrypted data for use.
- Same key (encryption/decryption)
- Used for enterprise cloud.

Algorithm	Working Structure	Key/Block Size (bits)	Known Attacks
DES	Feistel	56 (8 bits parity)/ 64	Brute-force attack
AES	Substitution-permutation	Up to 256/128	Side-channel attack
RC4	Random-permutation	Up to 2048/2064	NOMORE attack
RC5	Feistel	Up to 2040/128	Timing attack
RC6	Feistel	Up to 256/128	Brute force attack
Twofish	Feistel	Up to 256/128	Power analysis attack
Threefish	Tweakable block cipher/Non-Feistel	Up to 1024/1024	Boomerang attack
Serpent	Substitution-permutation	Up to 256/128	XSL and Meet-in-the-Middle attack
TEA	Feistel	Up to 128/64	Related-key attack
CAST-128	Feistel	Up to 128/64	Known-plaintext attack
GOST Block Cipher	Feistel	256/64	Chosen-key attack

Algorithm	Working Structure	Key/Block Size (bits)	Known Attacks
RSA	Factorization	Variable	Brute force and timing attack
Diffie-Hellman	Elliptic Curves/Algebraic	Variable	Man-in-the-Middle attack
YAK	Nondeterministic Finite automation (NFA)	Variable	Key share and key replication attack
MD5	Merkle-Damgard Construction	Variable	Collision attack
MD6	Merkle-Damgard Construction	Variable	Brute-force attack/ Birthday attack
SHA	Merkle-Damgard Construction	160/512	Collision attack
RIPEMD - 160	Merkle-Damgard Construction	Up to 320 /512	Collision attack
HMAC	Merkle-Damgard Construction	Variable	Brute-force attack

Tools:

BC Text Encoder (encrypt text, Public key)

PKI

- Public Key Infrastructure.
- Policies, Procedure to create, manage, distribute, use, store → digital certificate.

Components

- Cert Mangement System (distribute, Verify)
- Digital Certificate (online transaction)
- Validation Authority (stores certificate)
- Certification Authority (issue, Verify DC)
- User (request, use certificate)
- Registration Authority (verifier)

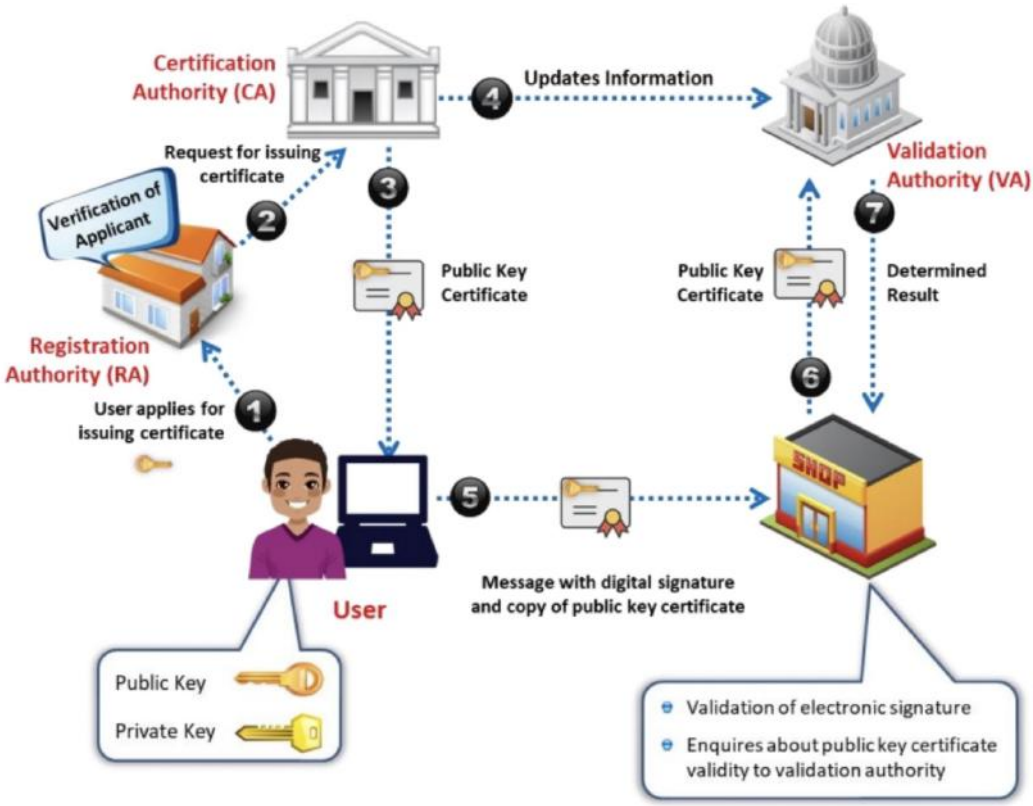


Figure 20.17: Public Key Infrastructure (PKI)

Self Signed

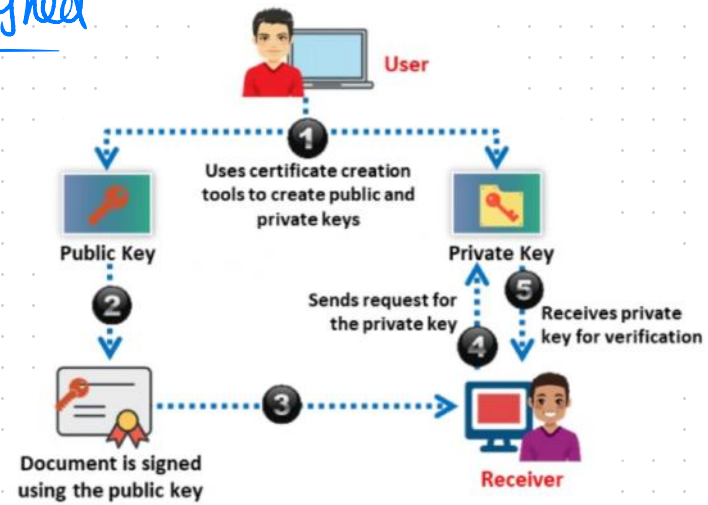


Figure 20.23: Process of generating self-signed certificates

Email Encryption

Digital Signature

- asymmetric cryptography.

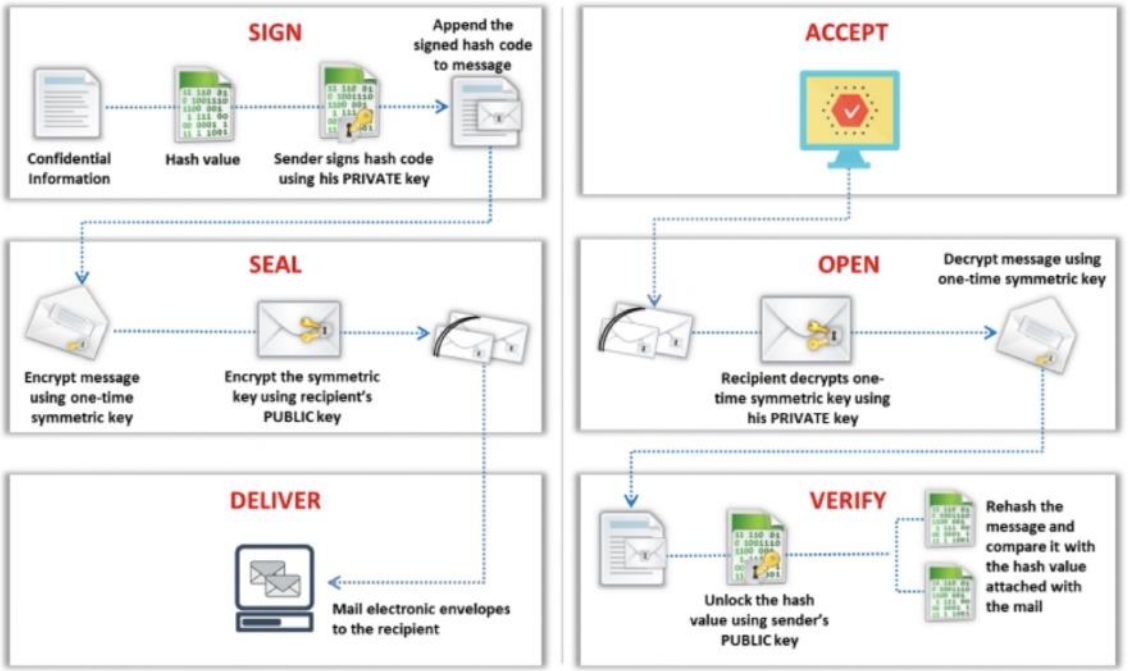


Figure 20.24: Using digital signature for email security

SSL

- RSA encryption for Internet transmission.

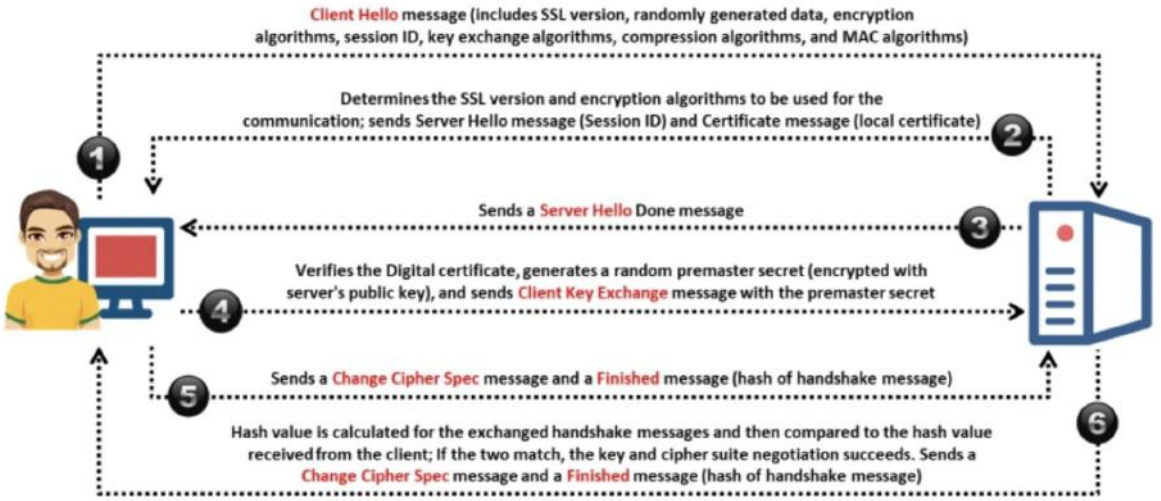


Figure 20.25: SSL handshake protocol flow

TLS

- establish secure connection ; RSA
- ensure privacy, integrity

Handshake Protocol (select algo, keys)

Record Protocol (DES)

two layers (TLS)

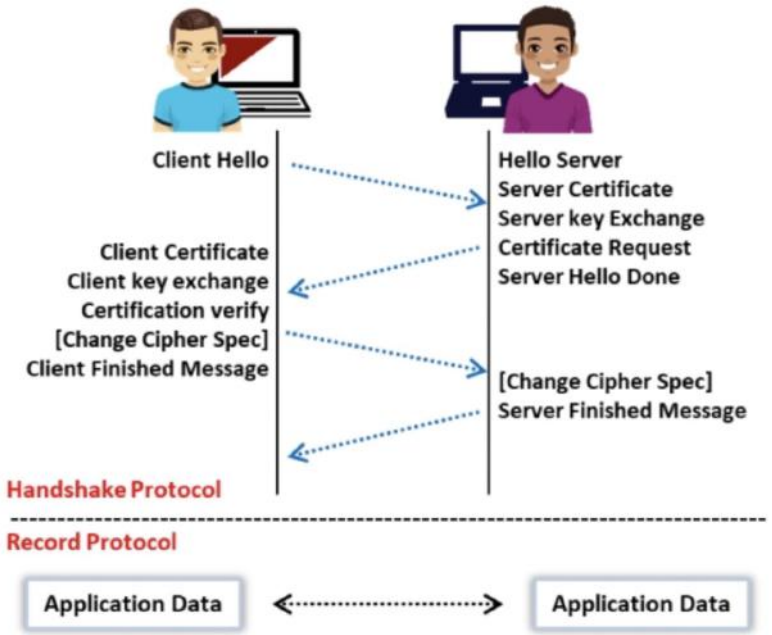


Figure 20.26: TLS handshake and record protocols

Toolkits

OpenSSL (SSL v2/v3, TLS v1)

Pretty Good Privacy

- Protocol to encrypt/decrypt data.
- Used for: compression, signing, messages, emails, files, directories.

- Hybrid Cryptosystem (convention, Public key)

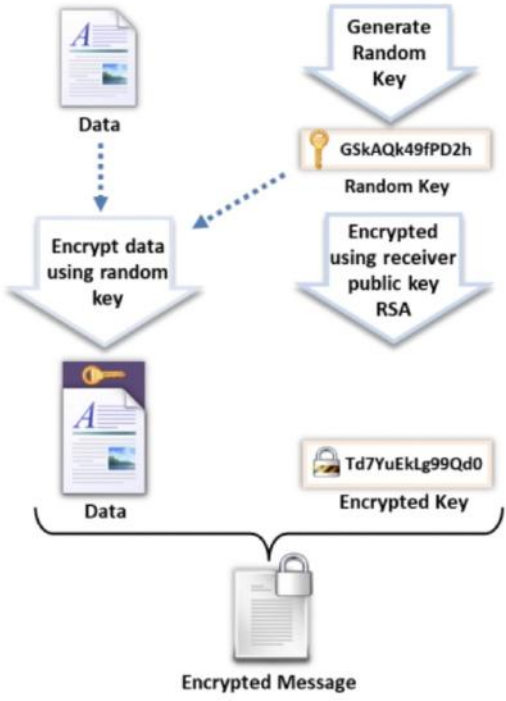


Figure 20.28: PGP Encryption

GPG

- GNU Privacy Guard.
- replacement of PGP (software)
- hybrid encryption (symm, asymm)
- S/MIME, SSH

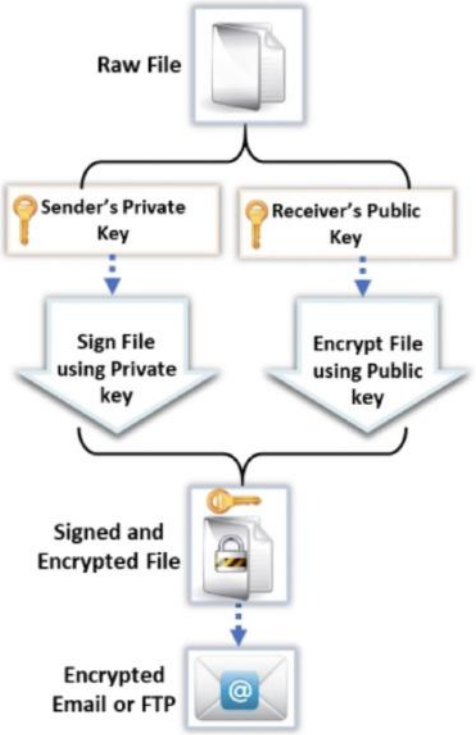


Figure 20.30: GPG Signing and Encryption

Figure 20.31: GPG Decryption and Verification

Web of Trust (WOT)

- trust model of PGP, OpenPGP, GnuPG.
- chain of CA networks who has ringe of public key.

Tools:

RMail (track, delivery proof, encrypt, signature)

Disk Encryption

Confidentiality (Privacy, hidden volumes, Password)

Encryption (Volume Encryption)

Protection (Blue ray, USB, Backup)

- VeraCrypt, Symantec Drive Encryption.
- BitLocker Encryption.

Cryptanalysis

- study of cipher, ciphertext, systems

Linear

- block cipher
- plaintext attack - linear approximation.
- pairs of cipher, plain → key found

Differential

- symmetric key
- difference of Input, Output
- works with chosen plain, known plain, ciphertext.

Integral

- Substitution Permutation network.

Methods

- Brute Force
- Frequency Analysis.
- Trickery & Deceit (social engineering)
- One Time Pad. (non repeat group of letter)

Attacks

Cipher only (know cipher, recover key)

Adaptive chosen plain. (choose plain from previous)

chosen plain (own plain)

Related key (two keys compare, relate)

Dictionary (plaintext dictionary)

Known plain (some knowledge - plain, key)

Chosen cipher. (own cipher)

Rubber hose (torture)

chosen key (breaks bit into $2^{n/2}$)

Timing (based on execution time)

MITM (Interception)

Brute-Force

Attack Scheme (large keys)

Brute Force

Success Factors (length, time, system)

DUHK attack

- Don't use Hard Coded keys
- obtains encryption keys to secure VPN

- ANSI → random number generator (RND) → Vulnerable.

Padding Oracle attack:

- Vaudenay attack
- exploits padding validation

DROWN attack

- cross protocol weakness.
- attacks SSLv3 / TLS
- Part of Online MITM attack

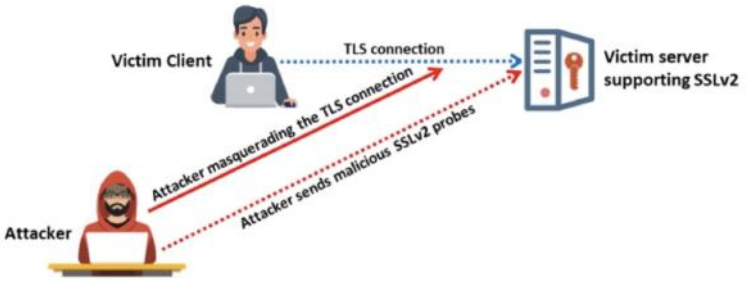


Figure 20.39: DROWN attack