Cryptography Basics and Applications

07th September 2021

Network Security and Performance Workshop - UPROUSE with LEARN

Thilina Pathirana

Based on and Credits: APNIC, APRICOT, NSRC, SANOG Security Tracks

Cryptography

- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Cryptanalysis = code breaking
- Cryptography is a function of plaintext and a cryptographic key

$$C = f(P, k)$$

Notation:

Plaintext (P)
Ciphertext (C)
Cryptographic Key (k)

Is it only for Messages?

- Digital Signatures
- Anonymous communication (TOR Network)
- Anonymous digital cash (Bitcoin etc)
  - Spending a digital coin without anyone knowing my identity
  - Buy online anonymously?
- Elections and private auctions - Finding the winner without knowing individual votes (privacy)

History

Caesar cipher, a mono-alphabetic system in which each character is replaced by the third character in succession

Vigenere cipher, a poly-alphabetic cipher that uses a 26x26 table of characters (14-15th Century)

Kerckhoff's Law (1883)

The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

In other words, the security of the system must rest entirely on the secrecy of the key.

Modern Crypto…

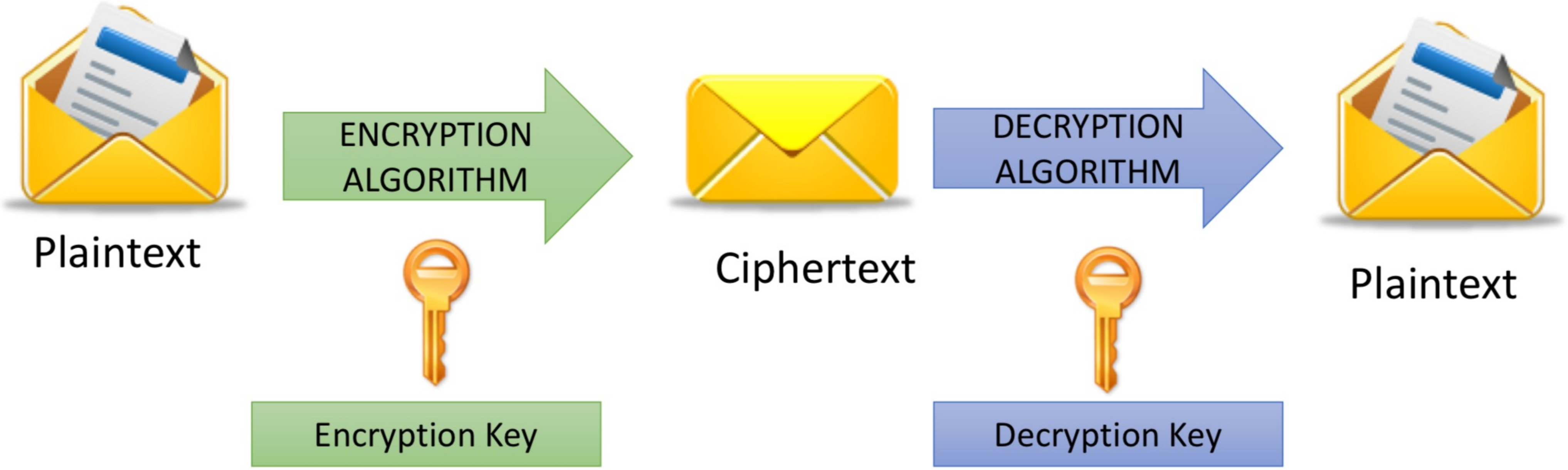
- Specifies the mathematical transformation that is performed on data to encrypt/decrypt
- Crypto algorithm is NOT proprietary
- Analyzed by public community to show that there are no serious weaknesses
- Explicitly designed for encryption

Try:

https://cryptii.com/

Encryption

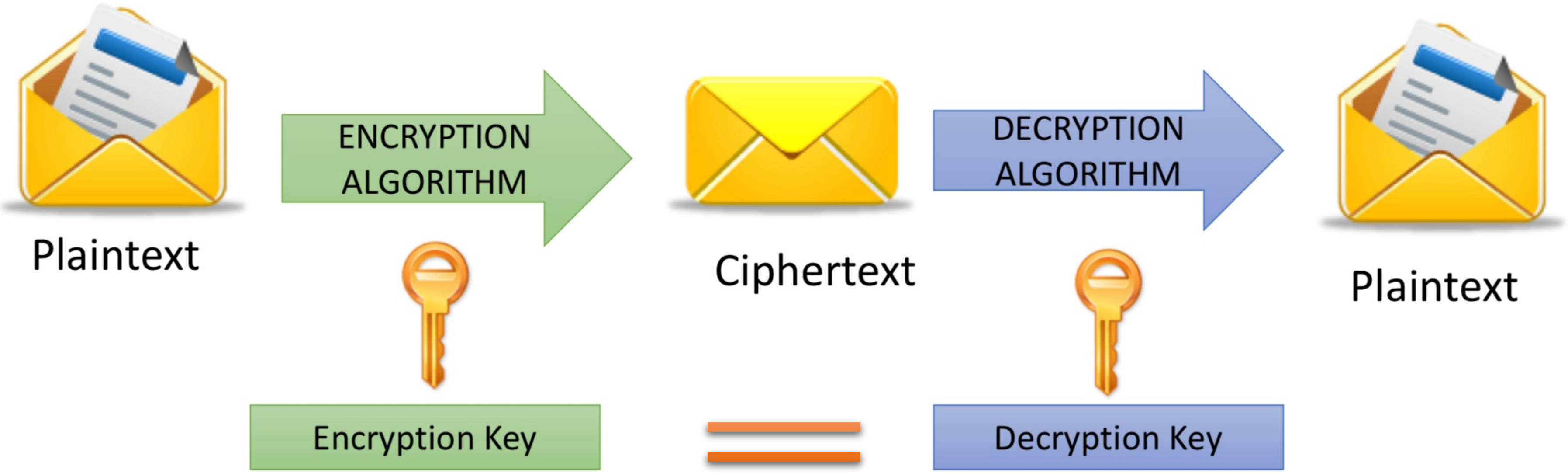
- Process of transforming plaintext to ciphertext using a cryptographic key
- In Application Layer – used in secure email, database sessions, and messaging
- In session layer – using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
- In the Network Layer – using protocols such as IPsec



Symmetric Key Encryption

- Uses a single key to both encrypt and decrypt information
- Also known as a secret-key algorithm, The key must be kept a “secret” to maintain security; This key is also known as a private key, but needs to be shared with all participating in the conversation
- Follows the more traditional form of cryptography with key lengths ranging from 40 to 256 bits.

Eg : DES, 3DES, AES, RC4, RC6, Blowfish

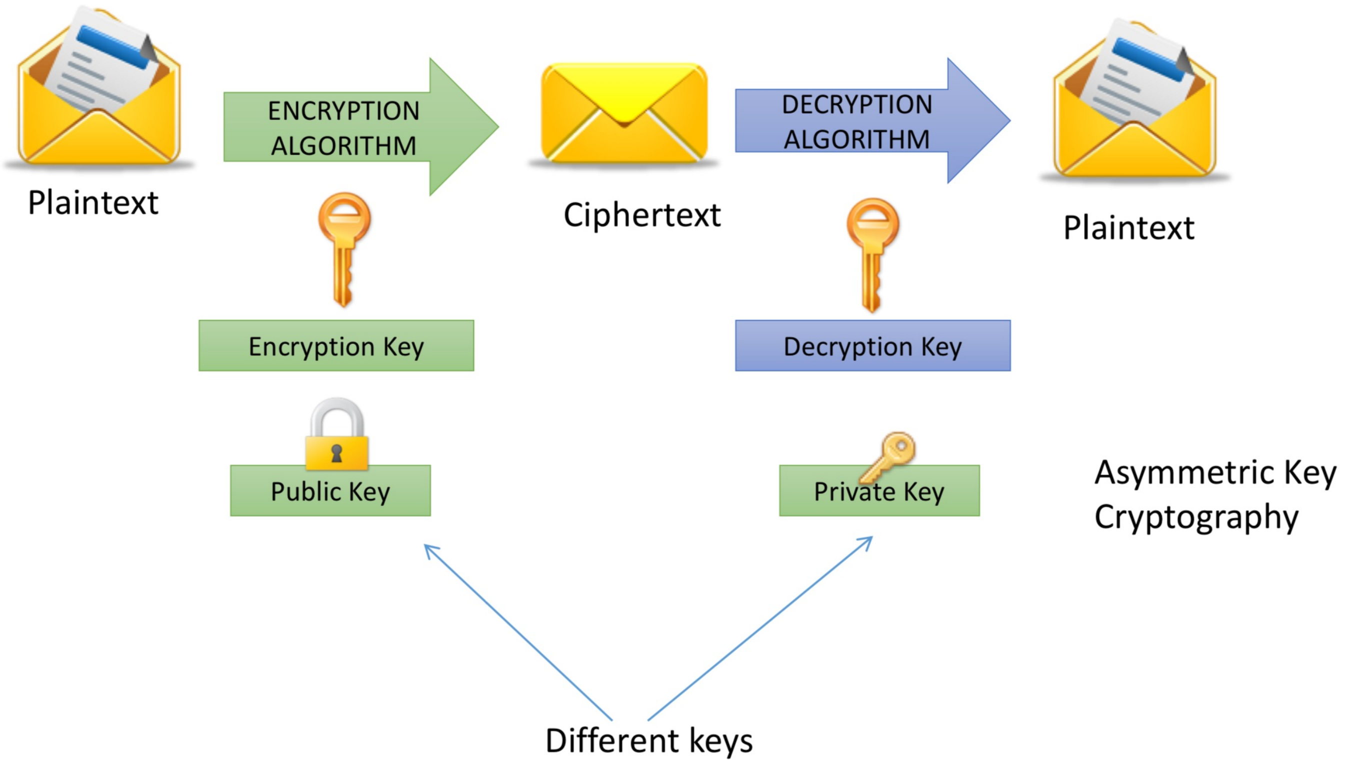


Symmetric Key Encryption

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, Used in most SSL implementations

Asymmetric Key Encryption

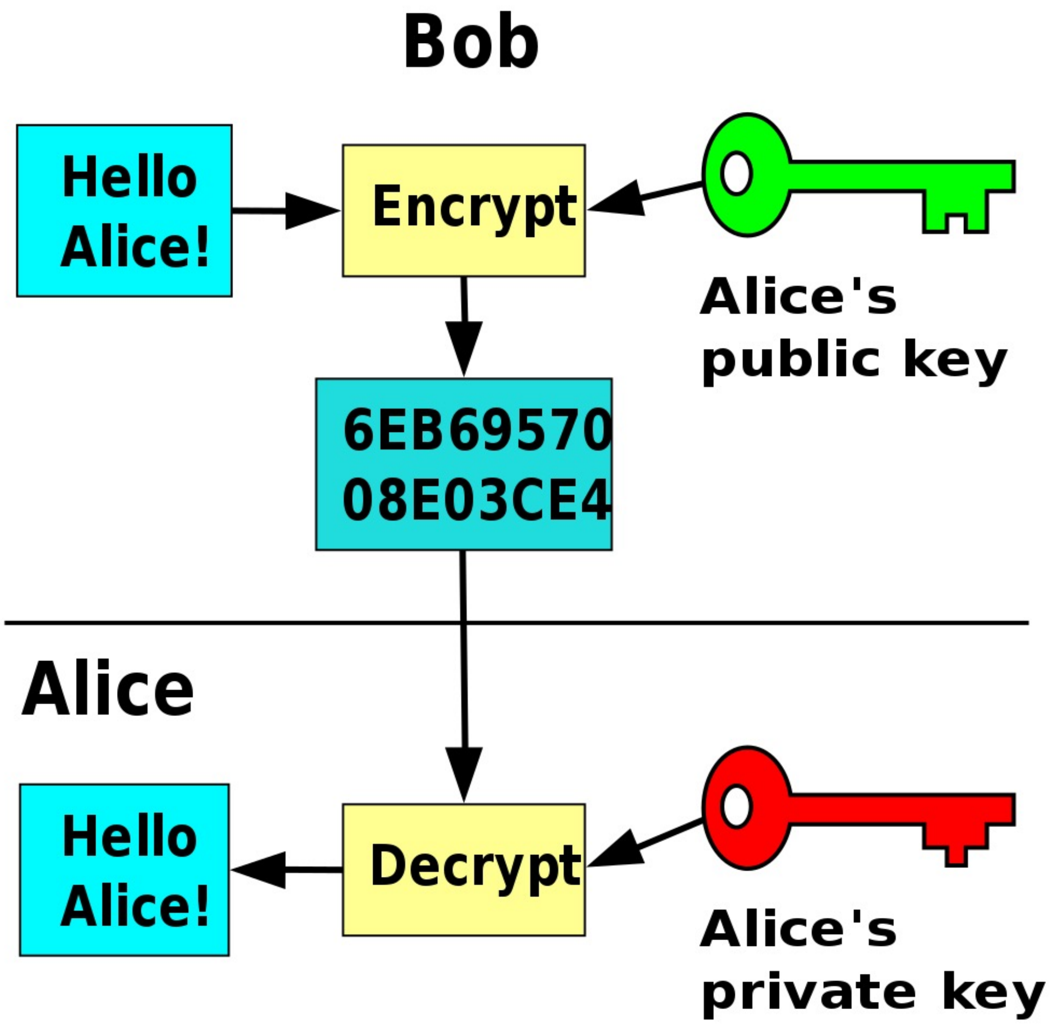
- Also called public-key cryptography
  - Keep private key to yourself and protected
  - Send/share the public key to anyone
- Separate keys for encryption and decryption (public and private key pairs)
- Examples:
  RSA,
  DSA,
  Diffie-Hellman,
  El Gamal,
  PKCS



Asymmetric Key Encryption

- A data encrypted by a public key can decrypt by the corresponding private key
- A data encrypted by a private key can decrypt by the corresponding public key
- Therefore, Keys are used as,
  - Public key for encryption
  - Private key for decryption
- Secret transmission of key for decryption is not required
- Every entity can generate a key pair and release its public key

Asymmetric Key Encryption



Asymmetric Key Encryption

Two most popular algorithms are RSA & El Gamal

RSA

- Developed by Ron Rivest, Adi Shamir, Len Adelman
- Both public and private key are interchangeable
- Variable Key Size (512, 1024, or 2048 bits)
- Most popular public key algorithm

El Gamal

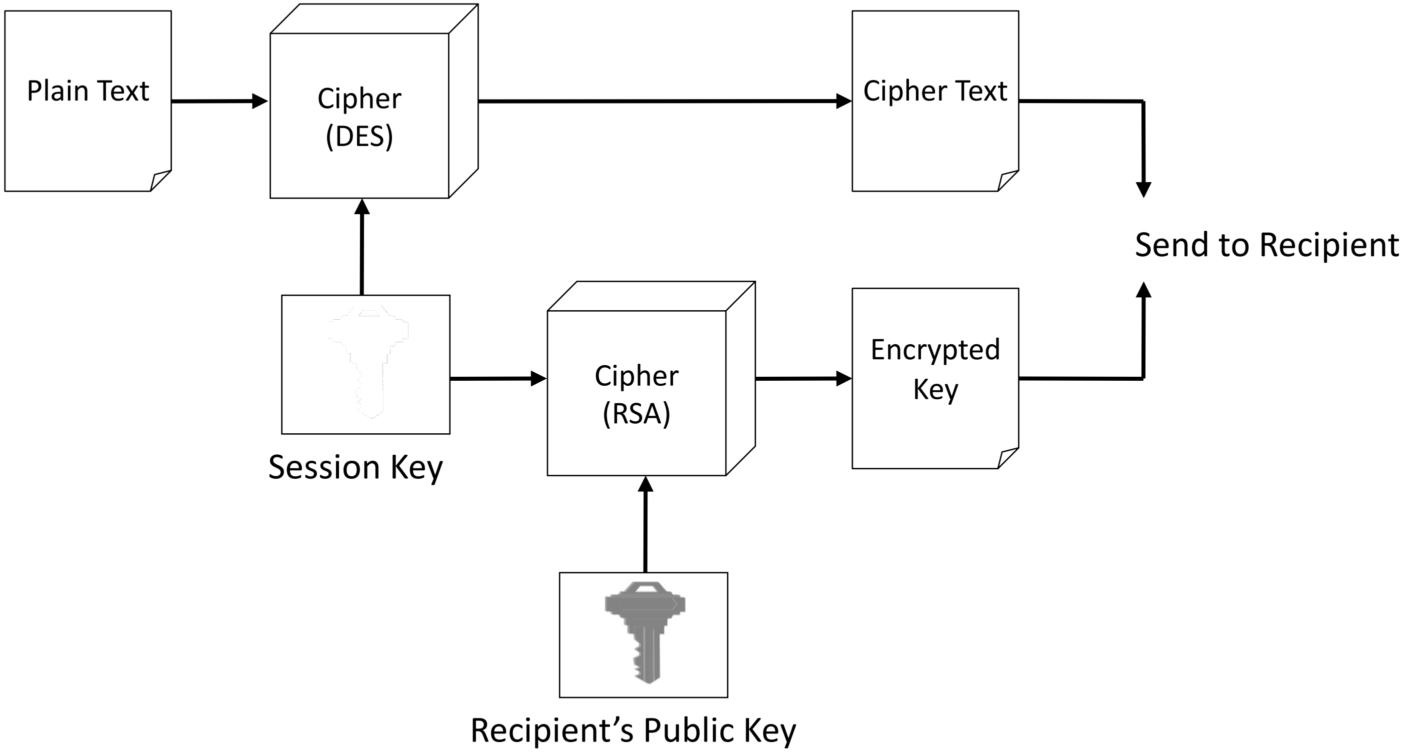
- Developed by Taher El Gamal
- Variable key size (512 or 1024 bits)
- Less common than RSA, used in protocols like PGP

Cryptographical Applications

Session Key Encryption

Used to improve efficiency

- Symmetric key is used for encrypting data
- Asymmetric key is used for encrypting the symmetric key



SSH

"SSH is a protocol for secure remote login and other secure network services over an insecure network." – RFC 4251

Secure channel between two computers

Provides data confidentiality and integrity

Many uses other than remote shell

SSH

SSH Transport Layer Protocol

- provides server authentication, confidentiality, and integrity services
- it may provide compression too
- runs on top of any reliable transport layer (e.g., TCP)

SSH User Authentication Protocol

- provides client-side user authentication
- runs on top of the SSH Transport Layer Protocol

SSH Connection Protocol

- multiplexes the secure tunnel provided by the SSH Transport Layer and User Authentication Protocols into several logical channels
- these logical channels can be used for a wide range of purposes
- secure interactive shell sessions
- TCP port forwarding
- carrying X11 connections

SSH

Step 1:
The client opens a connection to the server

Step 2:
Server sends

Its public host key

Another public key (``server key'') that changes every hour

The client compares the received host key against its own database of known host keys, Can decide to

Reject keys coming from unknown hosts

Accept them and store them in its database

SSH

Step 3:
The client

Generates a 256 bit random number using a cryptographically strong RNG (session key)

Picks an encryption algorithm among those supported by the server

Encrypts the session key using both the host key and the server key

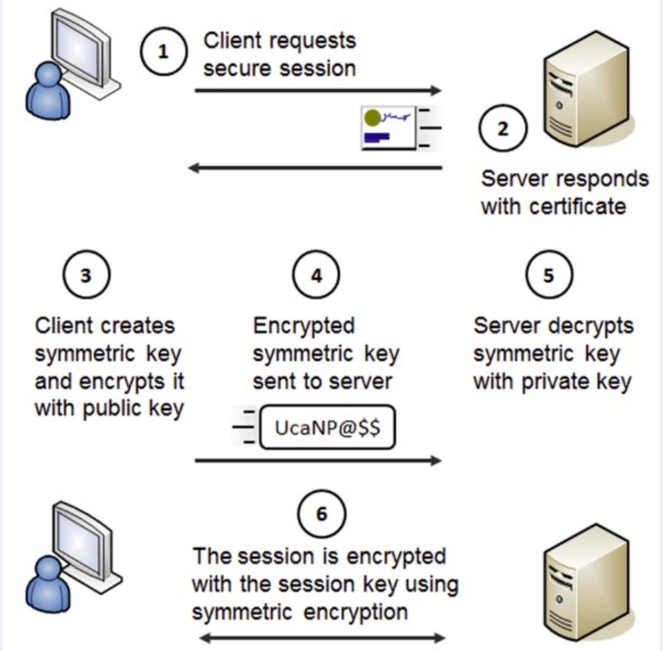
Sends the encrypted key to the server

SSH

Step 4:
Server decrypts the session key

Sends an encrypted confirmation to the client showing that it holds the proper private keys

Now client and server can start using transport-level encryption and integrity protection


1
Client requests secure session
2
Server responds with certificate
3
Client creates symmetric key and encrypts it with public key
4
Encrypted symmetric key sent to server
UcaNP@$$
5
Server decrypts symmetric key with private key
6
The session is encrypted with the session key using symmetric encryption

SSH User Authentication

Protocol assumes that the underlying transport protocol provides integrity and confidentiality (e.g., SSH Transport Layer Protocol)

the protocol has access to the session ID

the server should have a timeout for authentication and disconnect if the authentication has not been accepted within the timeout period

- recommended value is 10 minutes

the server should limit the number of failed authentication attempts a client may perform in a single session

- recommended value is 20 attempts

Several authentication methods are supported

- publickey
- password
- hostbased

SSH User Authentication

We Will look at multiple ways of User Authentication schemes during the tutorials

Message Digest

A message digest is a fingerprint for a document

Purpose of the message digest is to provide proof that data has not altered

Process of generating a message digest from data is called hashing

Hash functions are one way functions with following properties

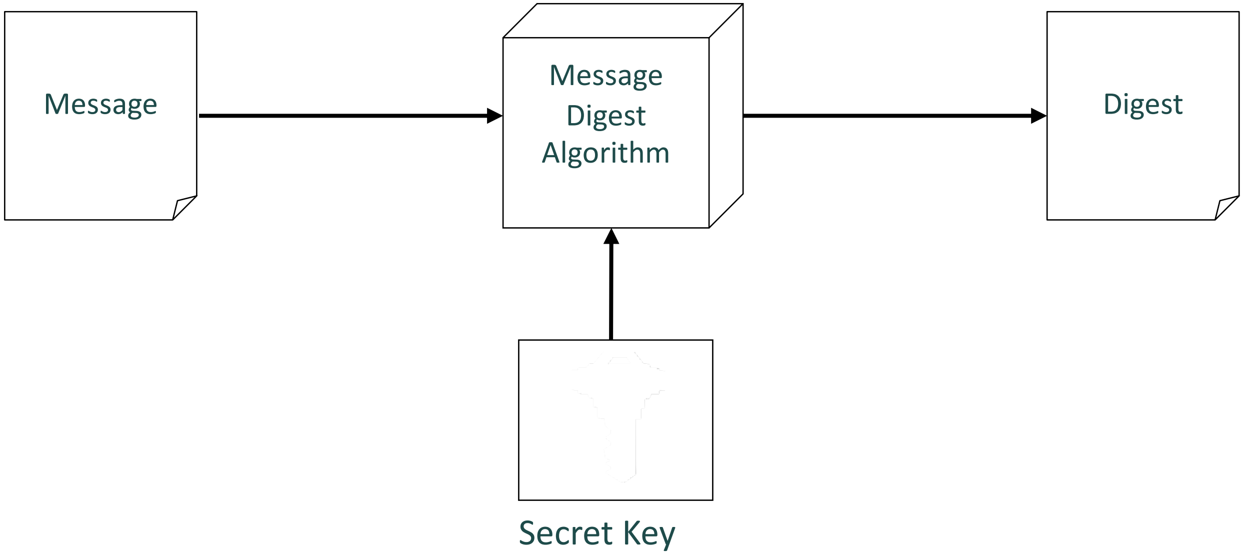
- Infeasible to reverse the function
- Infeasible to construct two messages which hash to same digest

Commonly used hash algorithms are

- MD5 – 128 bit hashing algorithm by Ron Rivest of RSA
- SHA & SHA-1 – 162 bit hashing algorithm developed by NIST

Message Authentication Codes (MAC)

- A message digest created with a key
- Creates security by requiring a secret key to be possesses by both parties in order to retrieve the message



Digital Signatures

A digital signature is a data item which accompanies or is logically associated with a digitally encoded message.

It has two goals

- A guarantee of the source of the data
- Proof that the data has not been tampered with

Digital signing is now used as an accepted means for producing signatures that are considered legally binding in many countries. When a digitally signed message has been received, the receiver has valid reason to believe that the message has originated from the designated sender, even if it has been relayed through a non-secure channel.

Therefore, In many cases, a digital signature is a legally accepted alternative to a handwritten signature or official seal certifying the authenticity of the signature

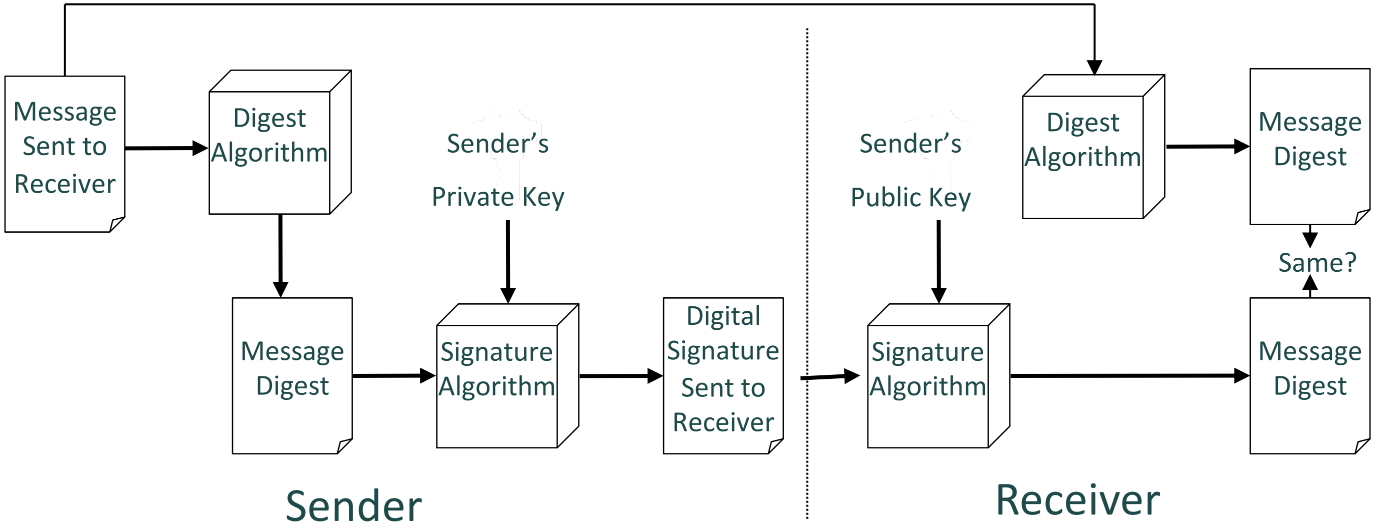
Digital Signatures

There are typically three algorithms involved with the digital signature process:

Key generation – This algorithm provides a private key along with its corresponding public key.

Signing – This algorithm produces a signature upon receiving a private key and the message that is being signed.

Verification – This algorithm checks for the authenticity of the message by verifying it along with the signature and public key.



Pretty Good Privacy - PGP

Let's say Bob want to send a secret message to Alice:

1. Alice has a private key and she has put its connected public key on her web page or a key management public site.
2. Bob download her public key.
3. Bob encrypt his secret message using Alice's public key and send it to her.
4. Only Alice can decode Bob's secret message because she's the only one with the corresponding private key.

Pretty Good Privacy is mostly concerned with the minutiae of creating and using public and private keys. You can create a public/private key pair with it, protect the private key with a password, and use it and your public key to sign and encrypt text.

Pretty Good Privacy - PGP

PGP builds trust upon a web of trust. You don’t need to trust the person.

What you need to check is the matching of the person and his/her public key(s)

- You can ask ID cards to confirm the person’s name which is usually included in the public key
- And fingerprint of the key to check if the public key you have is actually the key which the person distributed
- Another way trusting is using others trust to trust someone. If some other trusted person says he trusts that person, we can trust that person too. This is called the web of trust.
- Trust is represents by signing the trusted parties public key
- Meaning of someone signing another’s public key is that there is a trust built.

Web of Trust

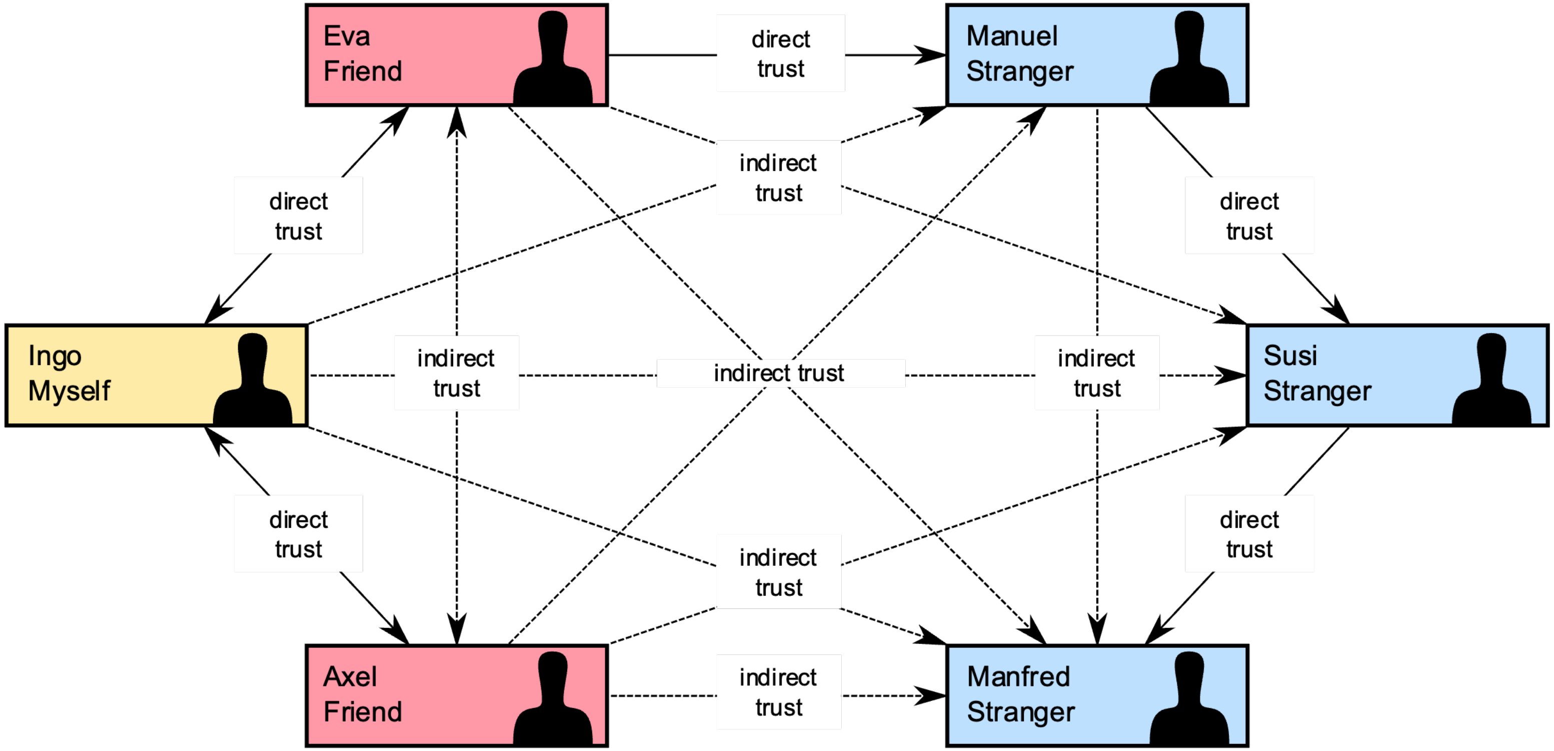
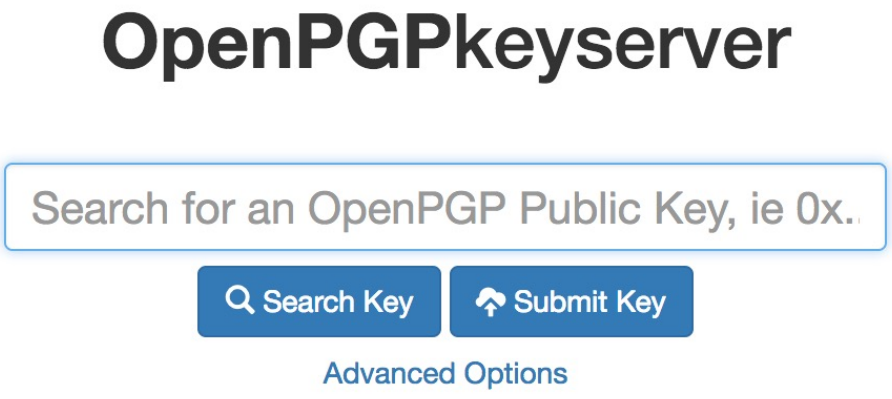
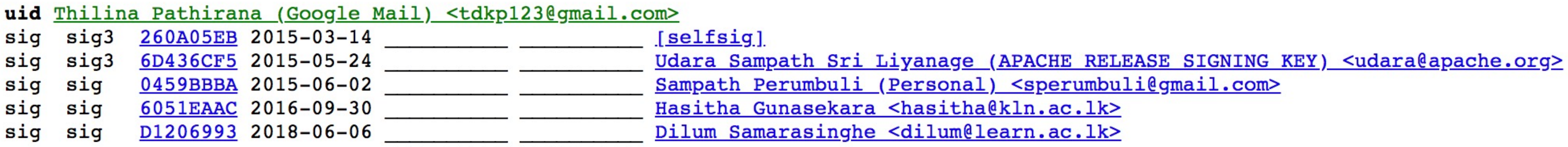


Image: Wikipedia

PGP Key servers

To make public keys available online, there are pools of public key servers that can be used by anyone. You can search or upload keys. All trusts will be shown as well. (pgp.mit.edu , pool.sks-keyservers.net)

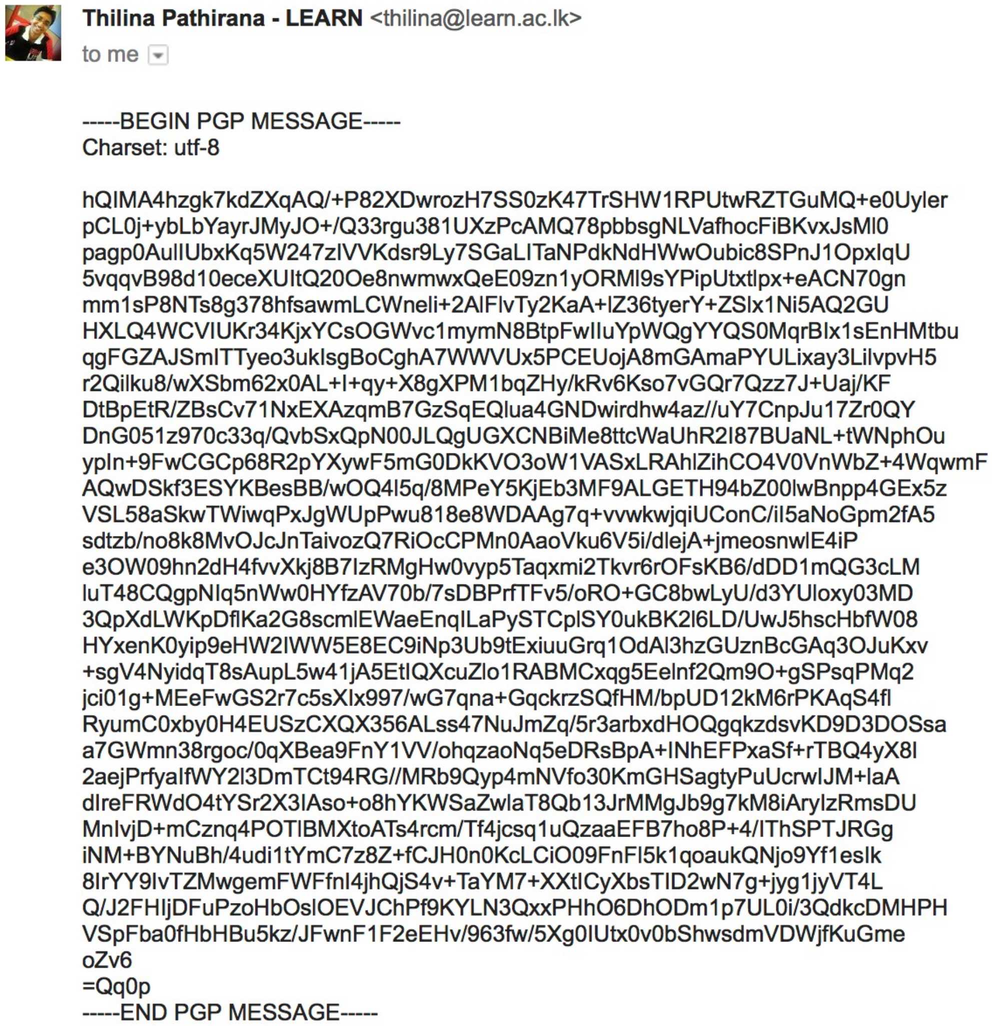




```
uid Thilina Pathirana (Google Mail) <tdkp123@gmail.com>
sig  sig3  260A05EB 2015-03-14 __________ __________ [selfsig]
sig  sig3  6D436CF5 2015-05-24 __________ __________ Udara Sampath Sri Liyanage (APACHE RELEASE SIGNING KEY) <udara@apache.org>
sig  sig   0459BBBA 2015-06-02 __________ __________ Sampath Perumbuli (Personal) <sperumbuli@gmail.com>
sig  sig   6051EAAC 2016-09-30 __________ __________ Hasitha Gunasekara <hasitha@kln.ac.lk>
sig  sig   D1206993 2018-06-06 __________ __________ Dilum Samarasinghe <dilum@learn.ac.lk>
```

Trusted parties

Example – PGP Encrypted Mail

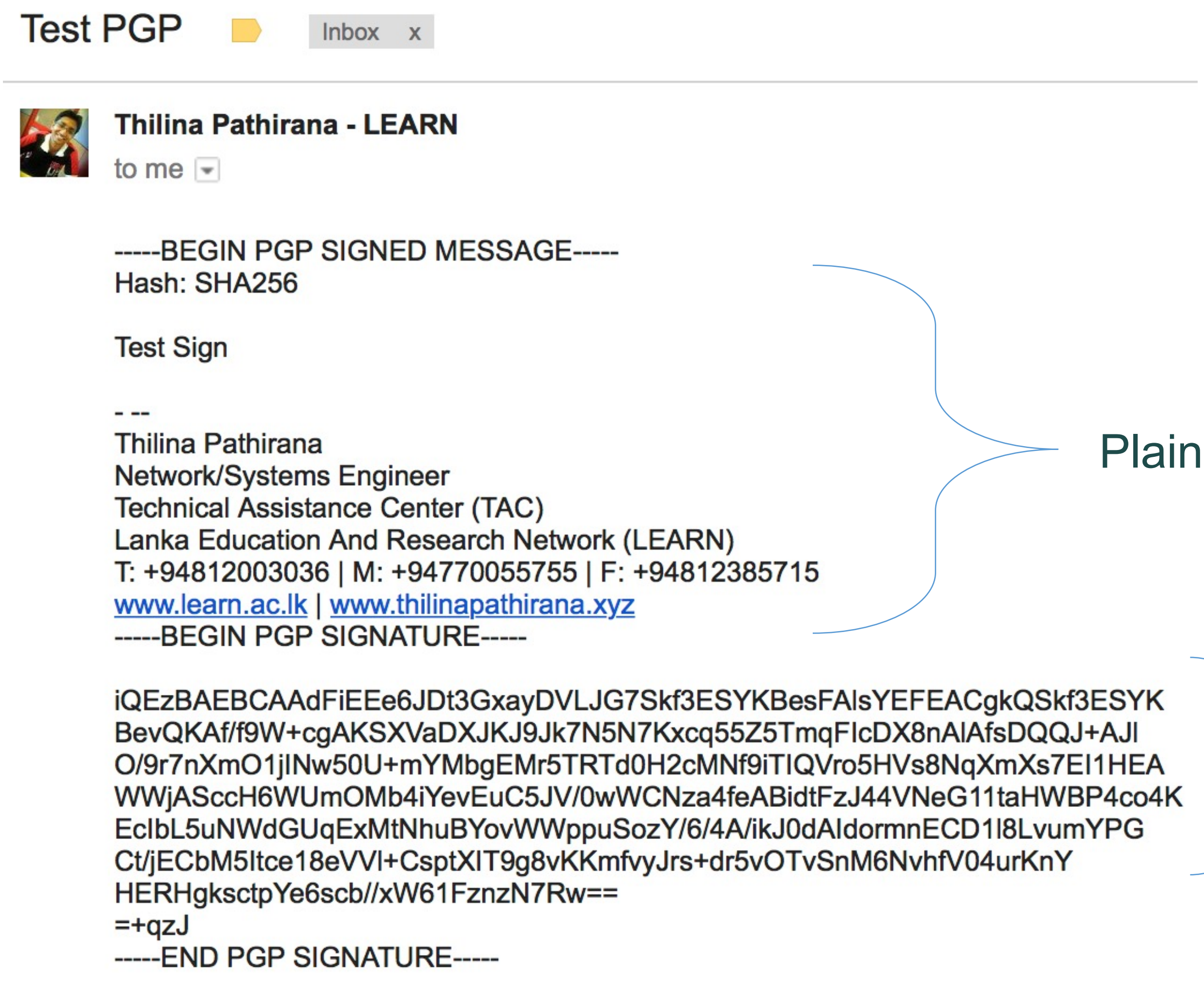


Thilina Pathirana - LEARN <thilina@learn.ac.lk>
to me

```
-----BEGIN PGP MESSAGE-----
Charset: utf-8

hQIMA4hzgk7kdZXqAQ/+P82XDwrozH7SS0zK47TrSHW1RPUtwRZTGuMQ+e0Uyler
pCL0j+ybLbYayrJMyJO+/Q33rgu381UXzPcAMQ78pbbsgNLVafhocFiBKvxJsMl0
pagp0AulIUbxKq5W247zIVVKdsr9Ly7SGaLITaNPdkNdHWwOubic8SPnJ1OpxIqU
5vqqvB98d10eceXUItQ20Oe8nwmwxQeE09zn1yORMl9sYPipUtxtlpx+eACN70gn
mm1sP8NTs8g378hfsawmLCWneli+2AlFlvTy2KaA+lZ36tyerY+ZSlx1Ni5AQ2GU
HXLQ4WCVIUKr34KjxYCsOGWvc1mymN8BtpFwlIuYpWQgYYQS0MqrBlx1sEnHMtbu
qgFGZAJSmITTyeo3ukIsgBoCghA7WWVUx5PCEUojA8mGAmaPYULixay3LilvpvH5
r2Qilku8/wXSbm62x0AL+I+qy+X8gXPM1bqZHy/kRv6Kso7vGQr7Qzz7J+Uaj/KF
DtBpEtR/ZBsCv71NxEXAzqmB7GzSqEQlua4GNDwirdhw4az//uY7CnpJu17Zr0QY
DnG051z970c33q/QvbSxQpN00JLQgUGXCNBiMe8ttcWaUhR2I87BUaNL+tWNphOu
ypIn+9FwCGCp68R2pYXywF5mG0DkKVO3oW1VASxLRAhlZihCO4V0VnWbZ+4WqwmF
AQwDSkf3ESYKBesBB/wOQ4l5q/8MPeY5KjEb3MF9ALGETH94bZ00lwBnpp4GEx5z
VSL58aSkwTWiwqPxJgWUpPwu818e8WDAAg7q+vvwkwjqiUConC/iI5aNoGpm2fA5
sdtzb/no8k8MvOJcJnTaivozQ7RiOcCPMn0AaoVku6V5i/dlejA+jmeosnwlE4iP
e3OW09hn2dH4fvvXkj8B7IzRMgHw0vyp5Taqxmi2Tkvr6rOFsKB6/dDD1mQG3cLM
luT48CQgpNIq5nWw0HYfzAV70b/7sDBPrfTFv5/oRO+GC8bwLyU/d3YUloxy03MD
3QpXdLWKpDflKa2G8scmlEWaeEnqILaPySTCplSY0ukBK2l6LD/UwJ5hscHbfW08
HYxenK0yip9eHW2IWW5E8EC9iNp3Ub9tExiuuGrq1OdAl3hzGUznBcGAq3OJuKxv
+sgV4NyidqT8sAupL5w41jA5EtIQXcuZlo1RABMCxqg5EeInf2Qm9O+gSPsqPMq2
jci01g+MEeFwGS2r7c5sXlx997/wG7qna+GqckrzSQfHM/bpUD12kM6rPKAqS4fl
RyumC0xby0H4EUSzCXQX356ALss47NuJmZq/5r3arbxdHOQgqkzdsvKD9D3DOSsa
a7GWmn38rgoc/0qXBea9FnY1VV/ohqzaoNq5eDRsBpA+INhEFPxaSf+rTBQ4yX8l
2aejPrfyaIfWY2l3DmTCt94RG//MRb9Qyp4mNVfo30KmGHSagtyPuUcrwlJM+laA
dIreFRWdO4tYSr2X3lAso+o8hYKWSaZwlaT8Qb13JrMMgJb9g7kM8iArylzRmsDU
MnIvjD+mCznq4POTIBMXtoATs4rcm/Tf4jcsq1uQzaaEFB7ho8P+4/IThSPTJRGg
iNM+BYNuBh/4udi1tYmC7z8Z+fCJH0n0KcLCiO09FnFl5k1qoaukQNjo9Yf1eslk
8IrYY9lvTZMwgemFWFfnl4jhQjS4v+TaYM7+XXtICyXbsTID2wN7g+jyg1jyVT4L
Q/J2FHIjDFuPzoHbOslOEVJChPf9KYLN3QxxPHhO6DhODm1p7UL0i/3QdkcDMHPH
VSpFba0fHbHBu5kz/JFwnF1F2eEHv/963fw/5Xg0IUtx0v0bShwsdmVDWjfKuGme
oZv6
=Qq0p
-----END PGP MESSAGE-----
```

Encrypted Message

Example – PGP Signed Mail

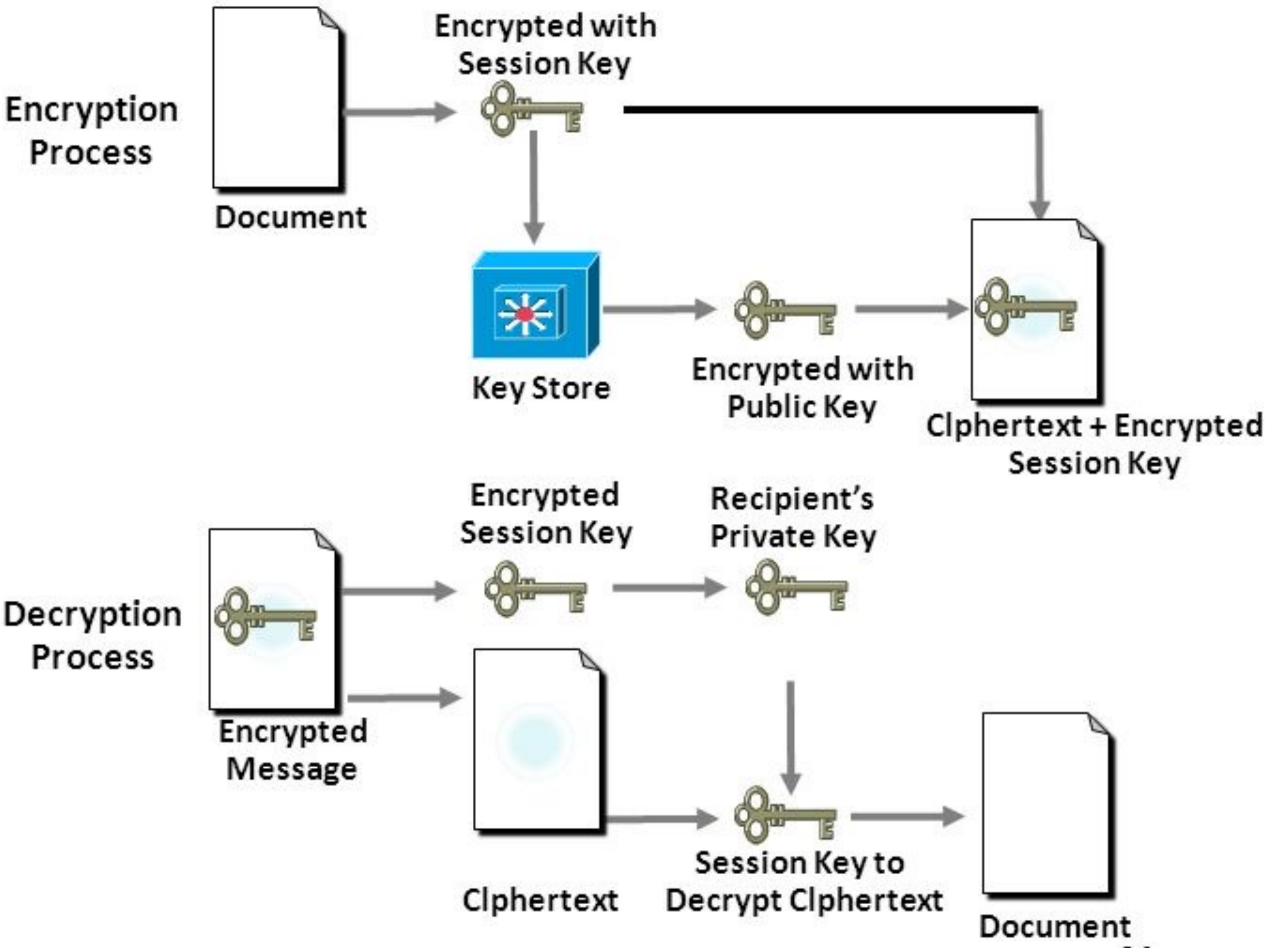


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Test Sign

- --
Thilina Pathirana
Network/Systems Engineer
Technical Assistance Center (TAC)
Lanka Education And Research Network (LEARN)
T: +94812003036 | M: +94770055755 | F: +94812385715
www.learn.ac.lk | www.thilinapathirana.xyz
-----BEGIN PGP SIGNATURE-----

iQEzBAEBCAAdFiEEe6JDt3GxayDVLJG7Skf3ESYKBesFAlsYEFEACgkQSkf3ESYK
BevQKAf/f9W+cgAKSXVaDXJKJ9Jk7N5N7Kxcq55Z5TmqFlcDX8nAlAfsDQQJ+AJl
O/9r7nXmO1jlNw50U+mYMbgEMr5TRTd0H2cMNf9iTIQVro5HVs8NqXmXs7EI1HEA
WWjAScCH6WUmOMb4iYevEuC5JV/0wWCNza4feABidtFzJ44VNeG11taHWBP4co4K
EclbL5uNWdGUqExMtNhuBYovWWppuSozY/6/4A/ikJ0dAldormnECD1l8LvumYPG
Ct/jECbM5ltce18eVVl+CsptXIT9g8vKKmfvyJrs+dr5vOTvSnM6NvhfV04urKnY
HERHgksctpYe6scb//xW61FznzN7Rw==
=+qzJ
-----END PGP SIGNATURE-----
```

Plain text Message

Signature –
Encrypted hash of the
Plain text Message

Example – PGP Process



Digital Certificate

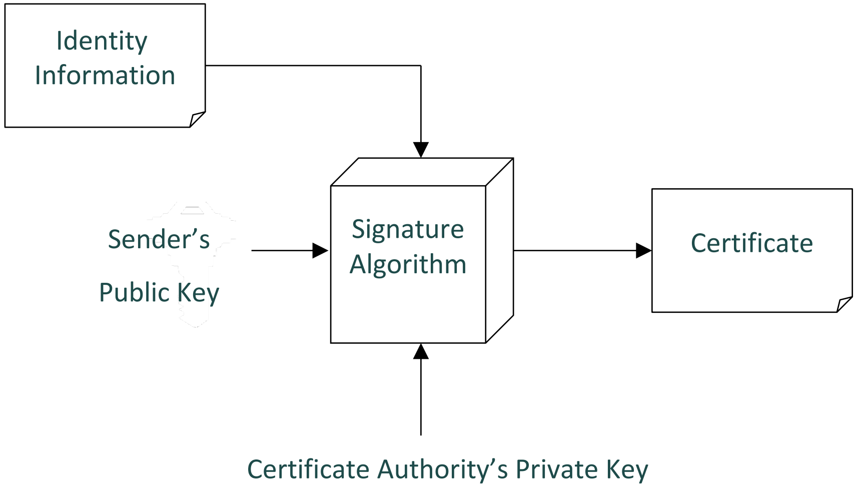
A digital certificate is a signed statement by a trusted party that another party's public key belongs to them.

- This allows one certificate authority to be authorized by a different authority (root CA)

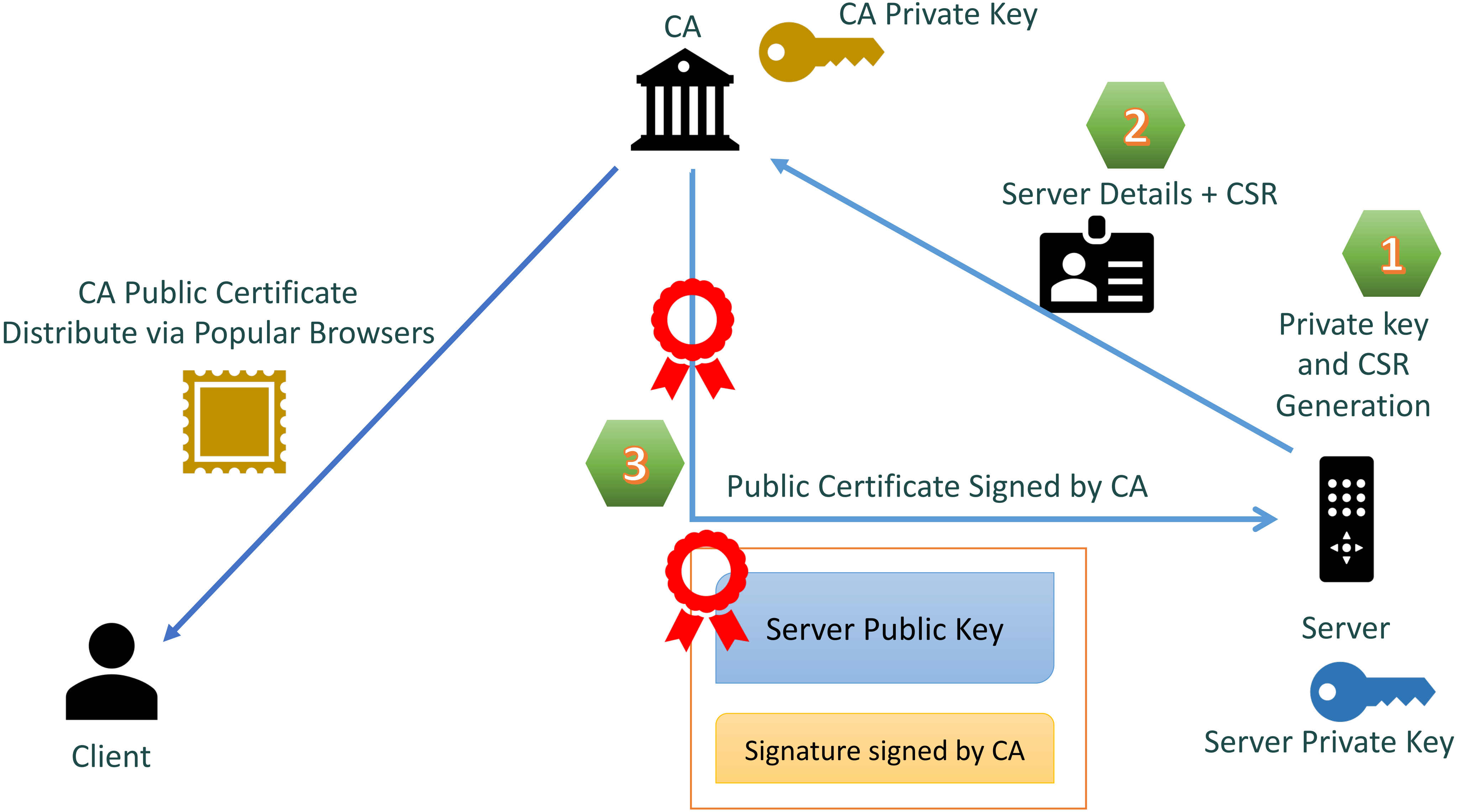
Top level certificate must be self signed

Any one can start a certificate authority

- Name recognition is key to some one recognizing a certificate authority
- Verisign is industry standard certificate authority

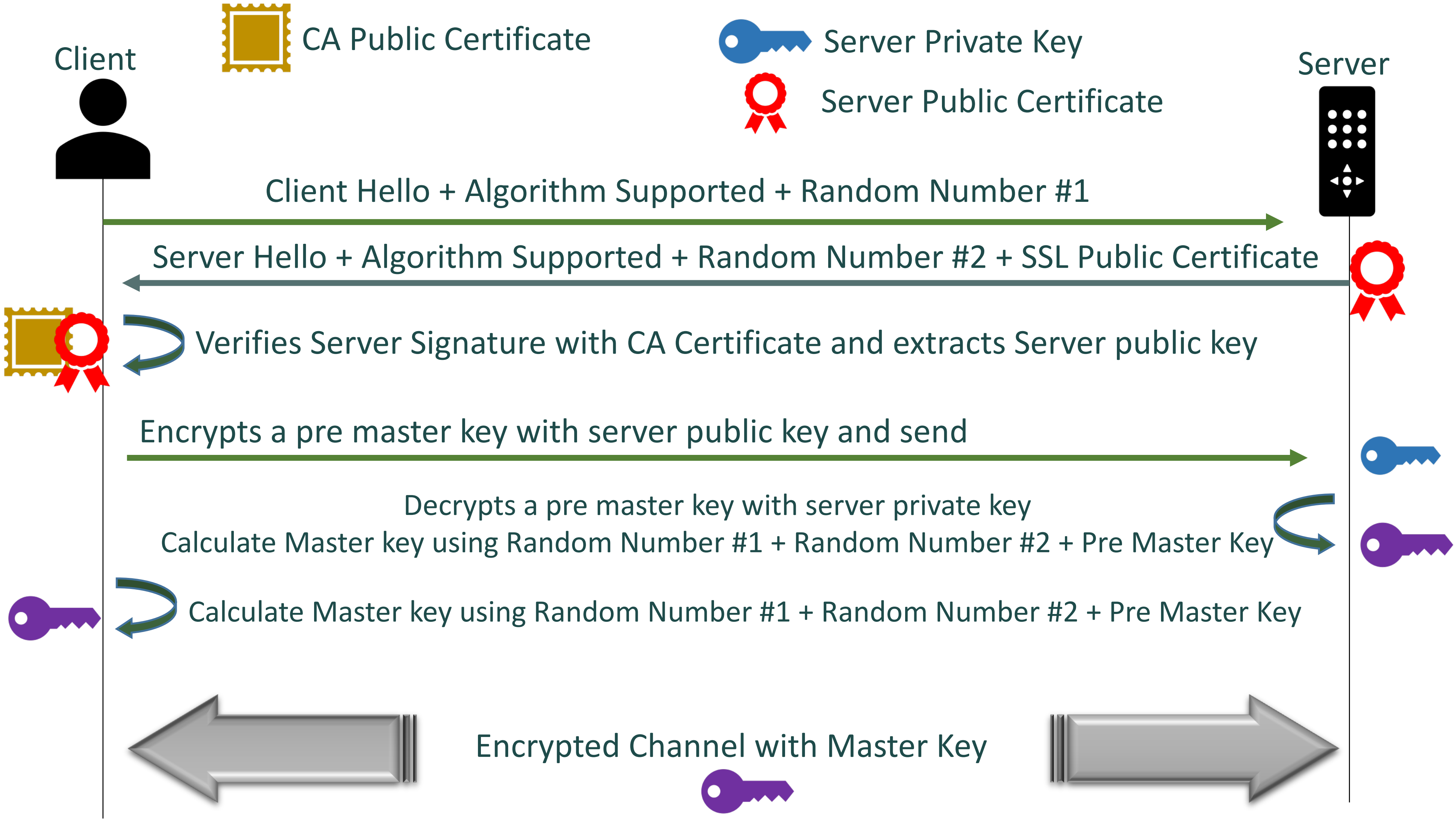


HTTPS Process – Certificate Creation



CA
CA Private Key
2
Server Details + CSR
1
Private key and CSR Generation
CA Public Certificate Distribute via Popular Browsers
3
Public Certificate Signed by CA
Server Public Key
Signature signed by CA
Server
Server Private Key
Client

HTTPS Process



CA Public Certificate

Server Private Key

Server Public Certificate

Client

Server

Client Hello + Algorithm Supported + Random Number #1

Server Hello + Algorithm Supported + Random Number #2 + SSL Public Certificate

Verifies Server Signature with CA Certificate and extracts Server public key

Encrypts a pre master key with server public key and send

Decrypts a pre master key with server private key
Calculate Master key using Random Number #1 + Random Number #2 + Pre Master Key

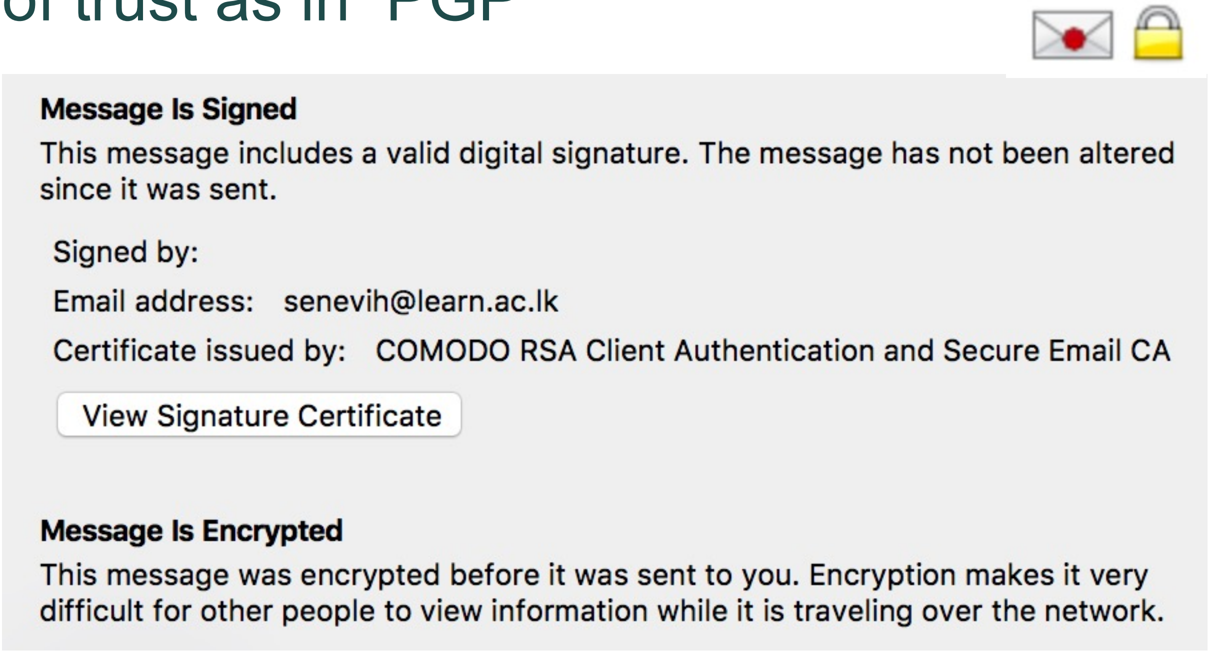
Calculate Master key using Random Number #1 + Random Number #2 + Pre Master Key

Encrypted Channel with Master Key

Secure/Multipurpose Internet Mail Extensions – S/MIME

This is again a similar protocol like PGP, but the difference is, there is a third party Certificate Authority who entrusts the public key.

When creating S/MIME certificates, you need to get signed your public certificate from a trusted Email CA, therefore we may not need the web of trust as in PGP



Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by:

Email address: senevih@learn.ac.lk

Certificate issued by: COMODO RSA Client Authentication and Secure Email CA

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.

Thank You