Network Security

- Principles of Network Security
- Cyber Attack
- Cyber Defence

Principles of Network Security

Network security is about protecting digital information resources and assets in the network

The primary goals are to ensure

Confidentiality (C)

- Data on the network can be **accessed** only by authorized users

Integrity (I)

- Data on the network can be **modified** only by authorized users

Availability(A)

- Data as well as services are **always** accessible or **available**
- Data can be static or in-transit

C.I.A. Triad

Consequences of compromised in Network Security

Compromised in Confidentiality	
Example	Consequence
Lose trade secrets, financial information to competitors	Revenue lost to competitor Financial loss
Compromised in Integrity	
Example	Consequence
Company's web site was vandalized by hackers replacing its original web contents	Lost of reputation Lost of Trust

Compromised in Availability	
Example	
Company network router was wrongly configured by administrator	Loss in productivity Loss of reputation Loss of revenue

Vulnerabilities, Threats and Attack

- Vulnerability
  - **Inherent weakness** in the design, configuration, implementation or management of a network and its resources that makes it susceptible to threats
- Threat
  - A threat is an activity (sequence of actions) with the **potential** for causing harm to the company's assets and resources
- Attack
  - Used a specific technique to **exploi**t a **vulnerability** in the network.
  - Active attacks are the **realization** of threats and involves **active work** done by the attacker
  - At least one of the goals of network security (C, I, A) is compromised

Cyber Attacks

- An intentional attempt to inflict damage (I), disrupt(A) or gain unauthorised access(C) to computer systems through the Internet

(1) Reconnaissance Phase :

Attacker gathers information about the target and scan for vulnerabilities

(2) Attack Phase:

Attacker carries out the actual attack and causes **damage** to the target.

(3) Cleanup Phase:

Attacker destroys evidence of the attack by clearing traces of the attack.

Vulnerable Code

SQLInjection.ipynb

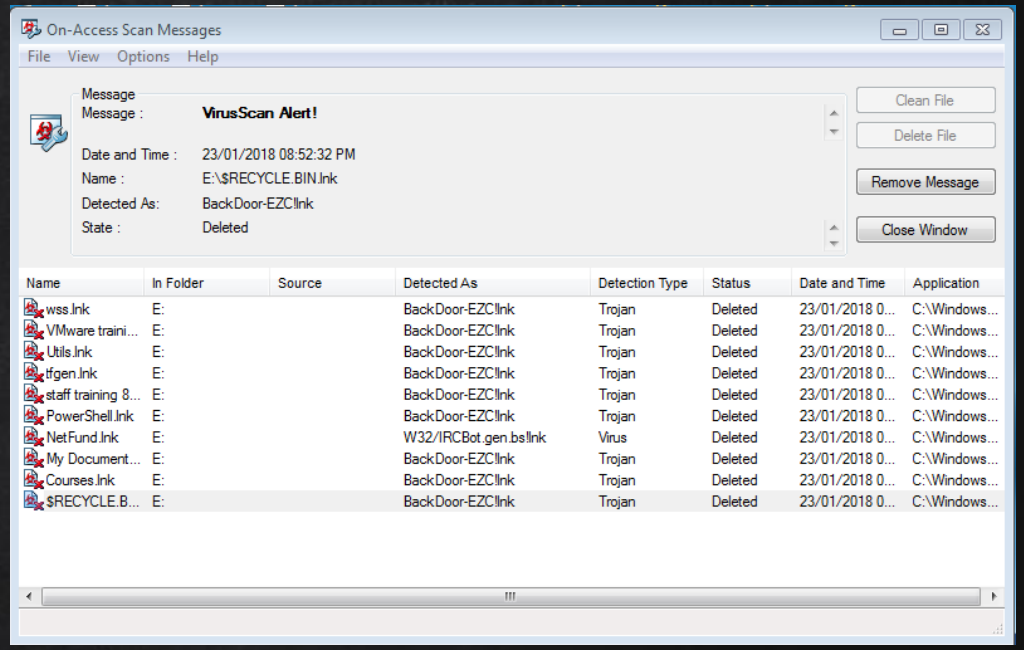
Malware

Malicious code, often referred to as **malware**, includes a wide range of software programs designed to harm, exploit, or otherwise compromise a computer system or network

Types	Definitions	Effects
Worms	A worm is standalone malware that replicates itself to spread across networks.	Can corrupt, delete, or steal data; often requires user action to spread.
Virus	A virus attaches itself to clean files and spreads through systems when the infected files are opened or executed.	Can corrupt, delete, or steal data; often requires user action to spread.
Trojans (Trojan Horses)	Disguises itself as a legitimate program or file to trick users into installing it.	Creates backdoors, steals data, or installs additional malware.

Preventing Cyber Attacks

- Install Anti-virus/Spyware program
- Install Personal Firewall
- Update software regularly
- Cookies management
- Be vigilant when responding to emails or submitting personal information to web sites
- Be diligent when importing module files from unknown sources into your code



Defending against Cyber Attack

- Authentication
- Authorisation
- Cryptography

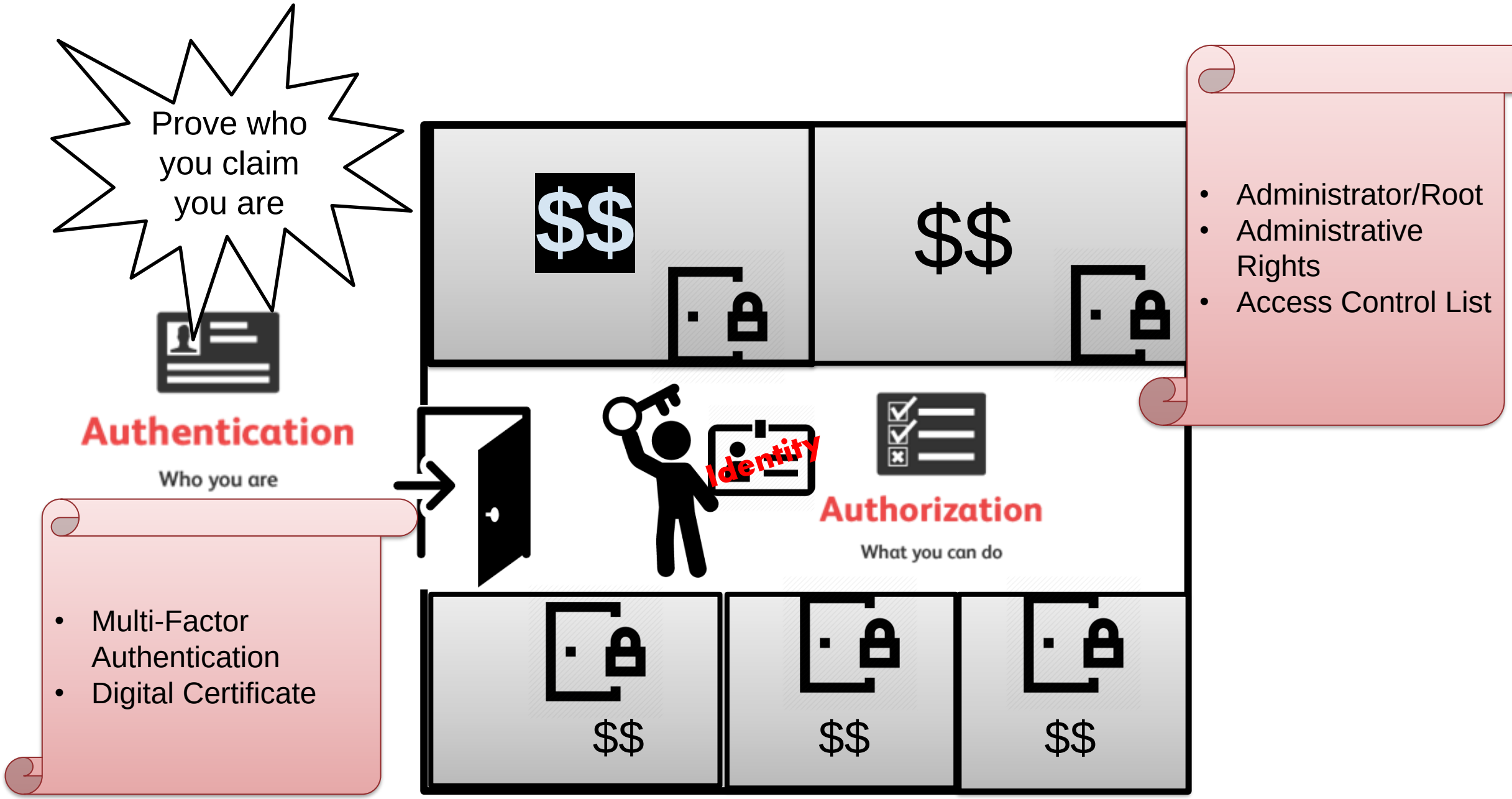
Authentication vs Authorisation

- **Authentication**
  - Process of **verifying** the **identity** of user
  - User needs to prove who he/she claims to be by providing evidence
  i. Something the user knows like login id and password
  ii. Something the user owns. Eg OTP (One Time Password) on mobile phone / token
  iii. Something unique that is measure from the user (Biometrics). Eg thumbprint, iris scan.

- Multi-factor Authentication uses 2 or more evidence

- **Authorisation (Access Control)**
  - Process of **granting a level of access** based on **the identity of the user**

Compartmentalised Access



Cryptography

The goals of cryptography are to secure communication by providing

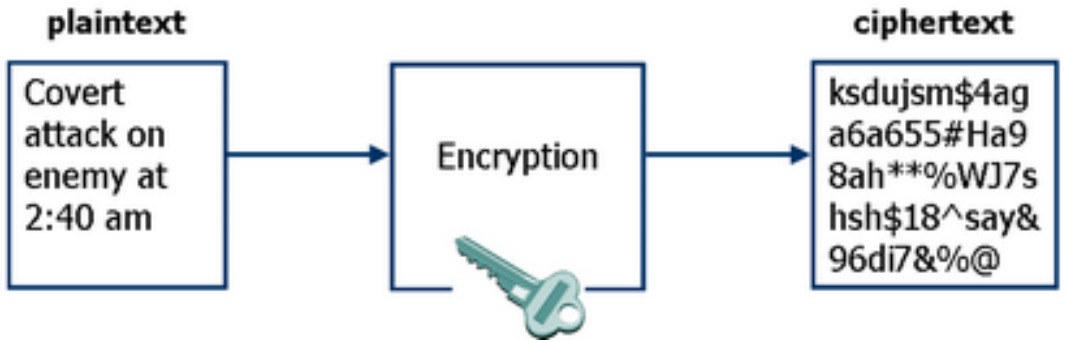
- Confidentiality
- Integrity
- Non-repudiation (cannot deny that an action has been performed)
- Authentications

These goals can be achieved with a combination of digital techniques such as encryption/decryption, hashing and digital signature

Encryption/Decryption

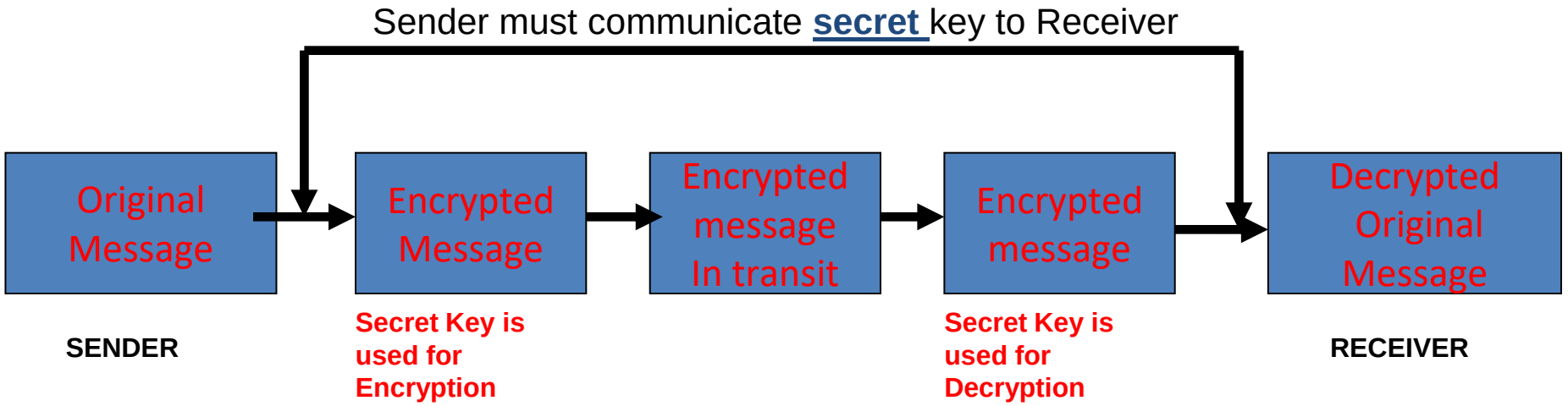
- Uses an algorithm and a key
- Primary Goal is Obfuscation
- *2 techniques*
  - *Symmetric and Asymmetric keys*

- *Encryption* – converting readable plaintext into non-comprehensible ciphertext



- *Decryption* – converting non-comprehensible ciphertext into readable plaintext

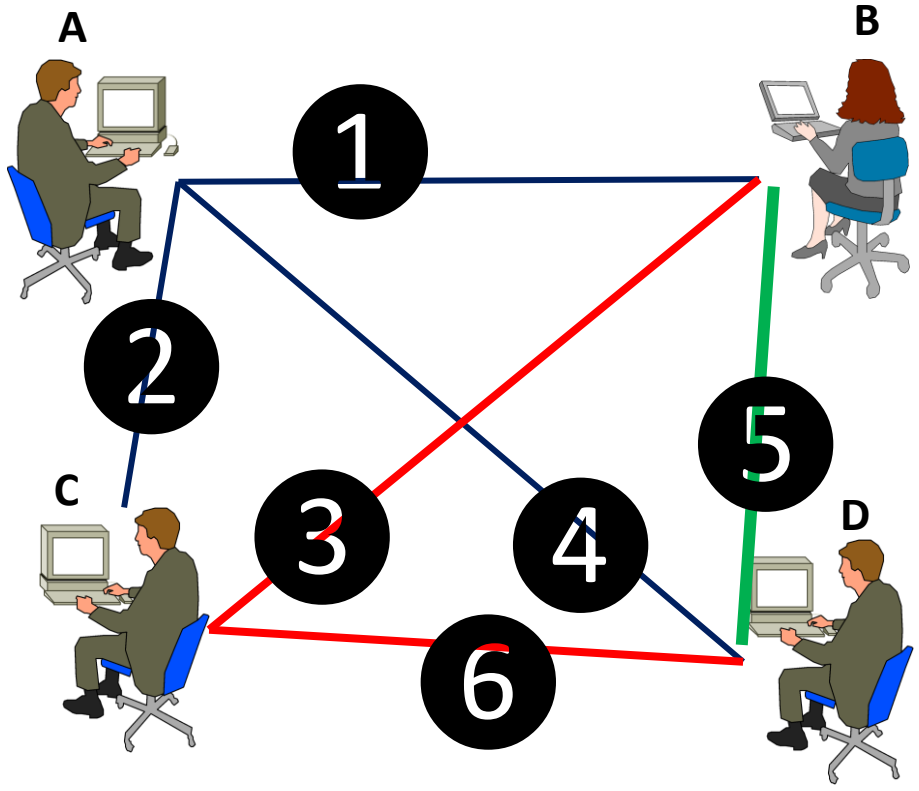
Symmetric-key Cryptography



Problem:
Distribution of secret keys

Advantage:
Symmetric encryption/decryption is fast

Symmetric cryptography – The Number of keys needed grows quadratically as the number of participants increase

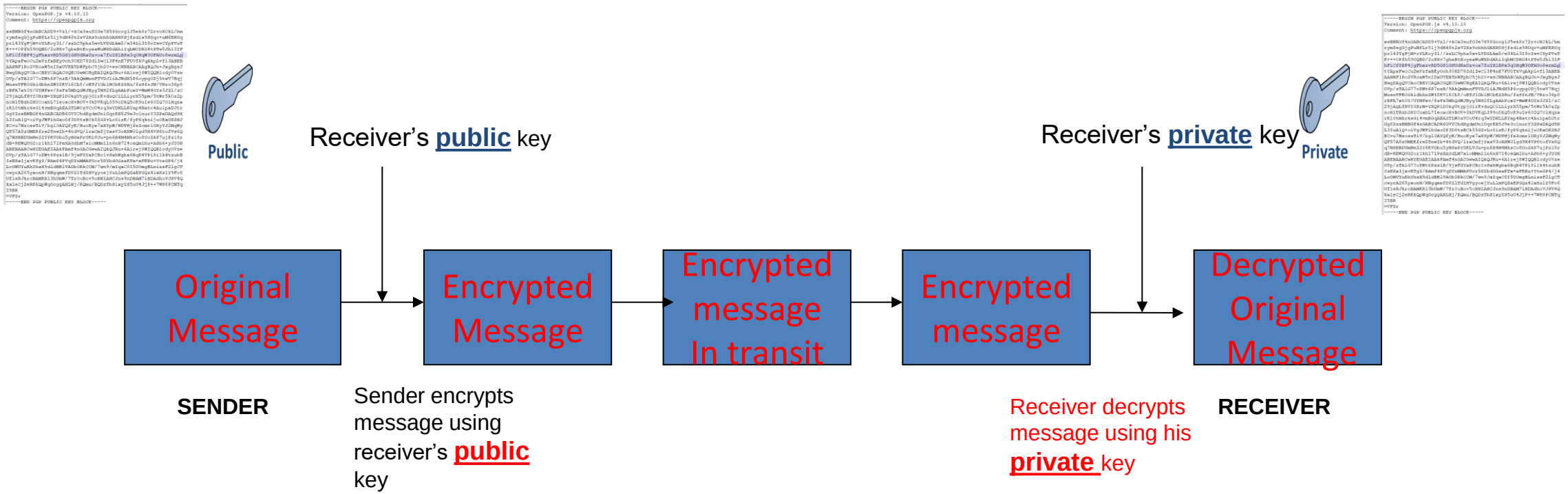


When 2 persons communicate, number of secret keys to maintain is 1
When 3 persons communicate, number of secret keys to maintain is 3
When 4 persons communicate, number of secret keys is 6

When n persons communicate the number of secret keys is the number of unique pairs of people, which is given by the combination formula

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

Asymmetric-key Cryptography



- Uses a **pair** of keys, public + private key for encryption and decryption
- **Secure** and manageable
- Problem is **slow encryption for large data**

Email scenario using Asymmetric Cryptography

- Alice wishes to send a secret message to Bob
- She looks up Bob's ___public___ key in a public directory
- Alice uses it to encrypt the message and sends it off
- Bob then uses his ___private____ key to decrypt the message and read it
- No one listening in can decrypt the message
- Anyone can send an encrypted message to Bob, but only Bob can read it (because only Bob knows Bob's private key)

Asymmetric Crypto using RSA

- The RSA (Rivest–Shamir–Adleman) Algorithm uses Asymmetrical Cryptography
- Demo / Practice
  a. Using PGP Online tool, generate a pair of keys download them as publicKey.txt and privateKey.txt
  b. Publish your public key in the Message Board padlet by uploading the file, keep your private key secret
  c. Use your friend's (Recipient) public key to encrypt a secret message for him/her.
     - Copy the public key from the padlet post)
  d. Copy the generated encrypted text and **save it in a file, encrypted.txt**
  e. Create a post in padlet (make sure you address the person) and **upload** the encrypted.txt file. **. (You cannot paste the encrypted text directly in the post)**
  f. Decrypt any secret messages received using your private key.

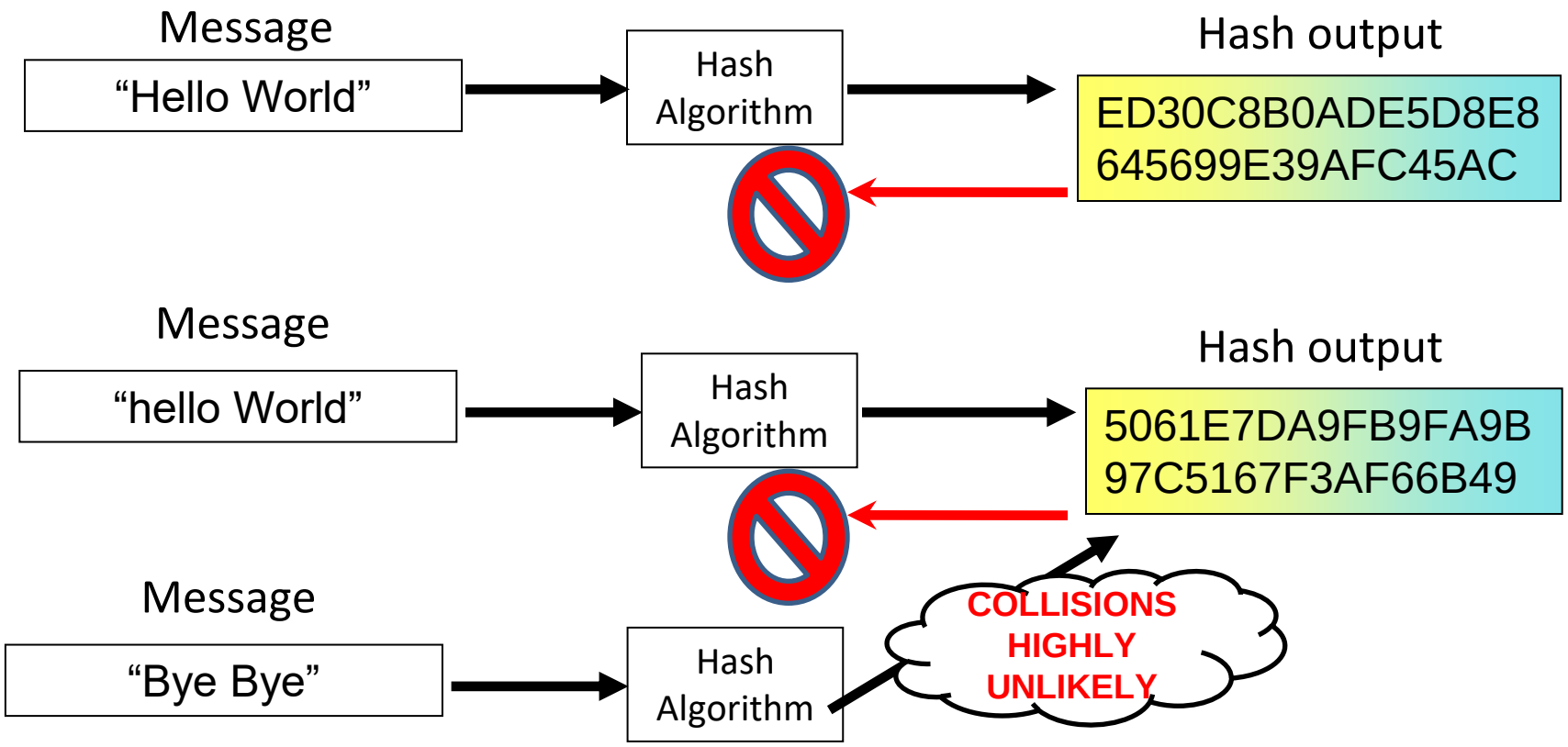
Tools PGP Online : https://onlinepgp.com/

Message Board: https://for.edu.sg/cz2a-padlet

(DO NOT USE)
Public Key Store: https://keys.openpgp.org/

Cryptography Hash Functions

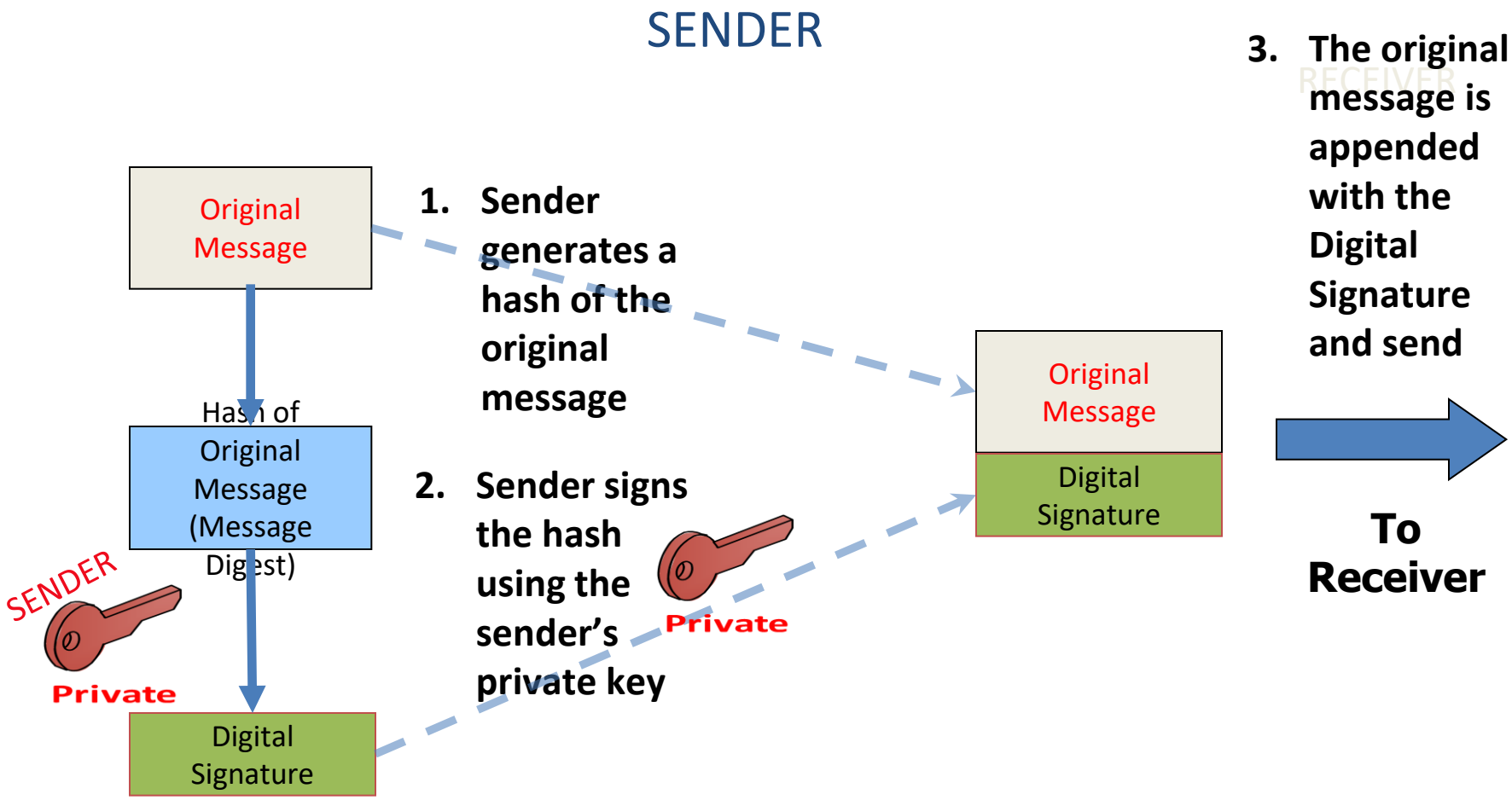
- One-way Function
  - **Non reversible**
- Maps input data of **any size** to a **fixed sized** output known as a digest or hash
- A tiny **change** in the input message produces a drastic change in the hash output
- The output is designed to make collisions computationally infeasible
- Examples of **Cryptography Hash Algorithm**: MD5 (Broken), SHA1(broken), SHA256 (most commonly used)



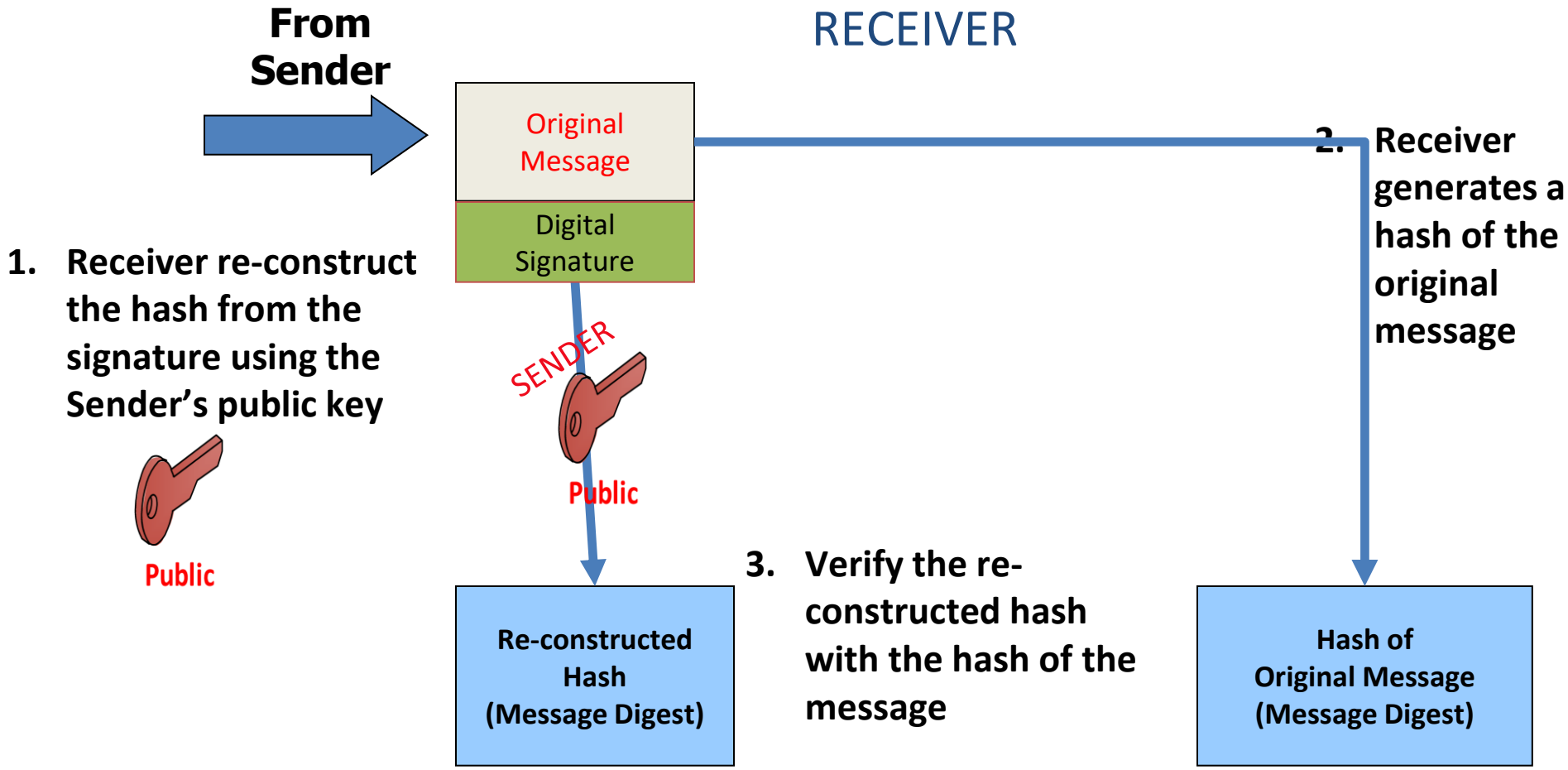
Digital Signature

- A digital signature serves the same purpose as a handwritten signature
- Digital signatures provide:
  - Authentication. The person digitally signing the message is really who he claims to be.
  - Non-repudiation. Signer cannot deny that he did not sign the document
  - Integrity. The data was sent and received without any alteration or modification

Signing a digital message with a Digital Signature



Verifying a Digital Signature



Verifying a Digital Signature

The Sender refers to the owner of the public key used during the verification process

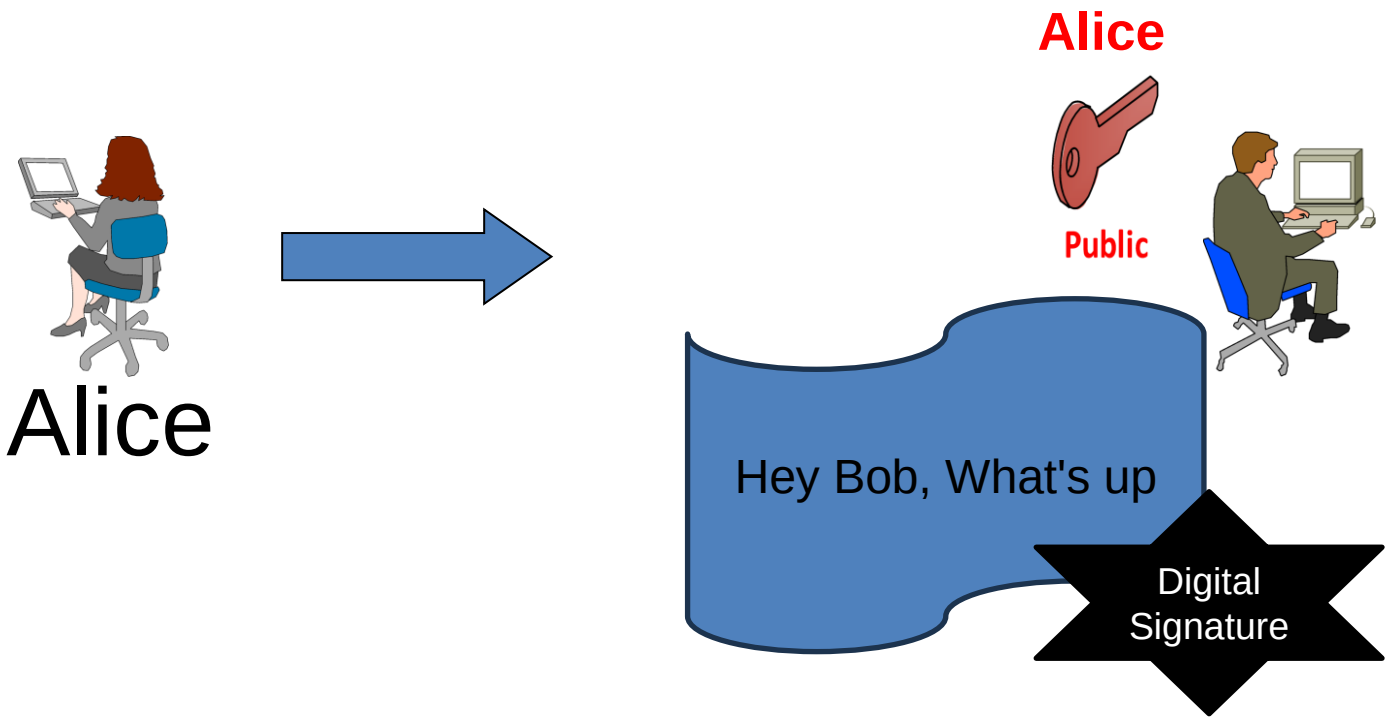
IF the verification returns True

- Authenticated Sender. The sender is authenticated
- Non-repudiation. Sender cannot deny that he did not sign the message.
- Integrity. The data was sent and received without any alteration or modification since a hash of a altered message will give a different output

IF the verification returns False

- Failed Authentication. The sender did not send the message
- Repudiation . Sender can deny sending the message
- Failed Integrity. Message was modified

How can you trust the public key of Alice belongs to Alice ?



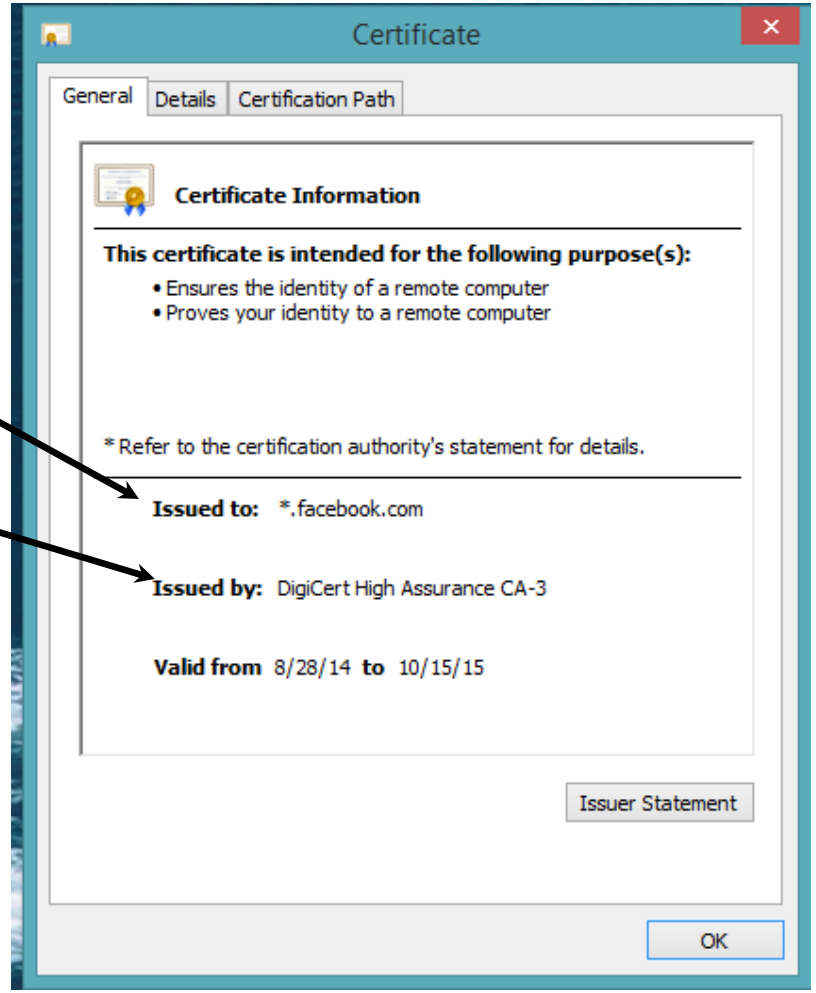
Or the web site
https://www.google.com.sg you are
browsing is really google ?

Public Key Infrastructure (PKI)

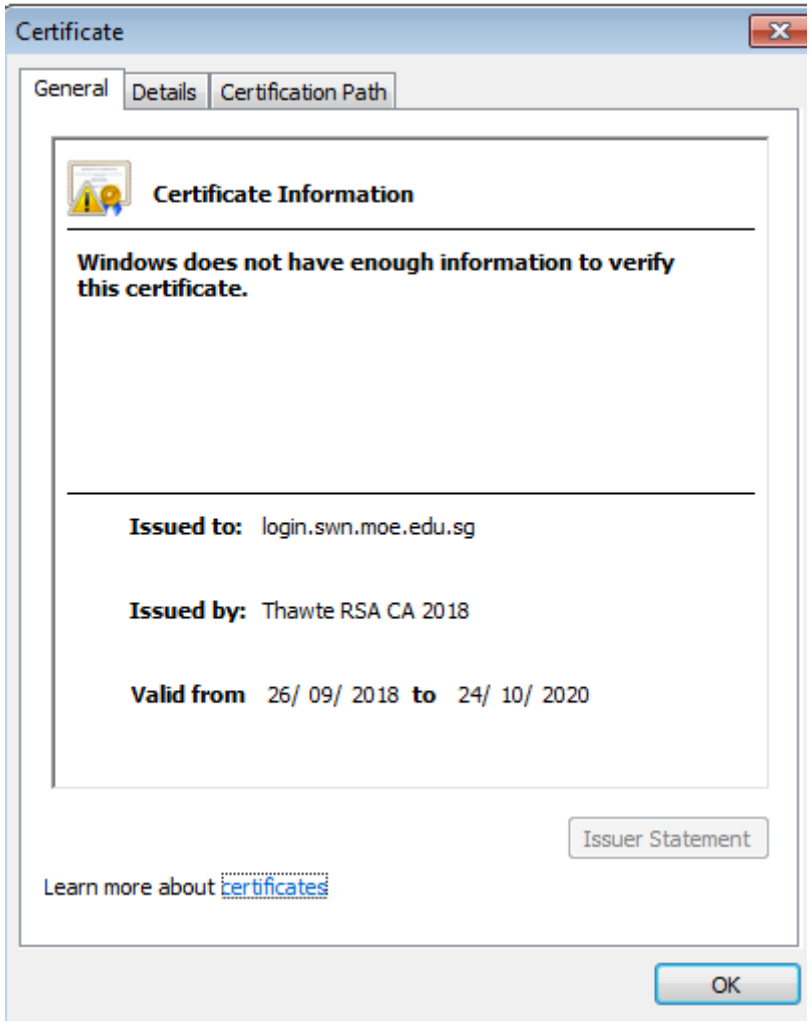
- Public keys are used to uniquely identify a user or computer.
- We can use them to send encrypted contents to a recipient or to verify the identity of a sender.
- A public key infrastructure supports the **distribution** and **identification** of public encryption keys, enabling users and computers to **securely** exchange data over an **untrusted network** such as the Internet.
- A PKI consists of the following elements
  - Certificate
  - Certificate Authority (CA)
  - Certificate Store

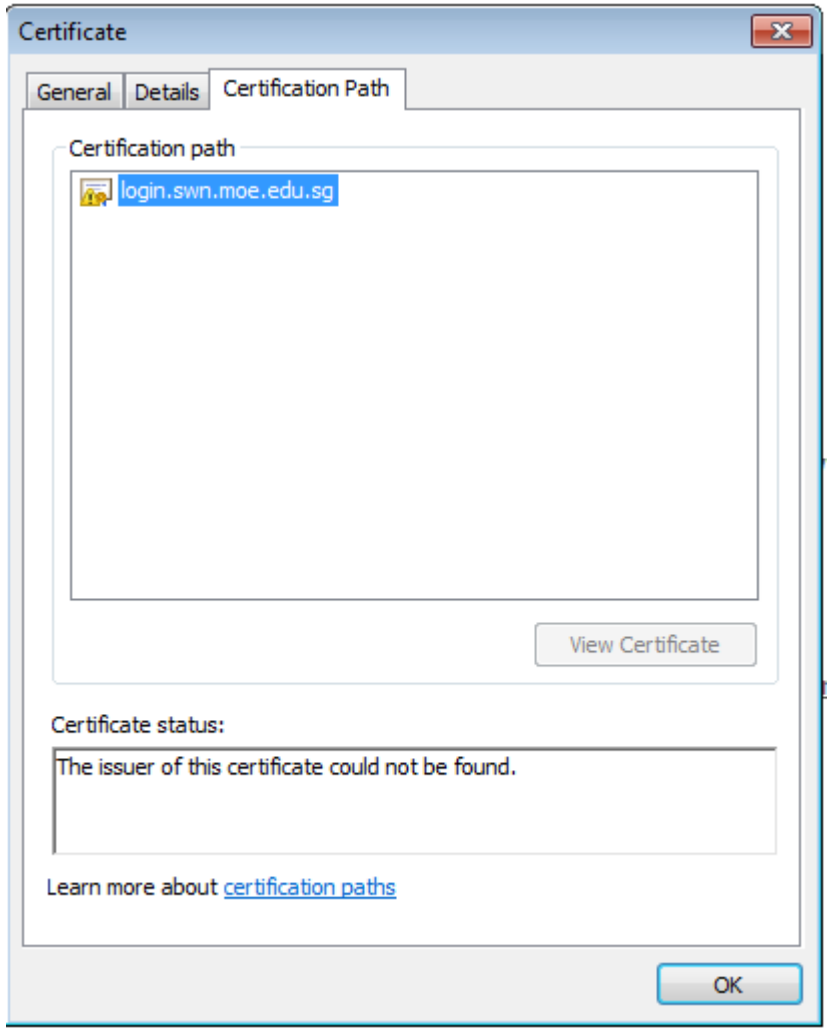
Digital Certificate

- A digital certificate contains the following information
  - Subject's (user or computer) identity
  - Issuer's identity (CA)
  - Valid Period
  - Public key of the subject
- A digital certificate maps a subject (person or computer) to a public key
- Guaranteed by the Issuer



Invalid Certificate





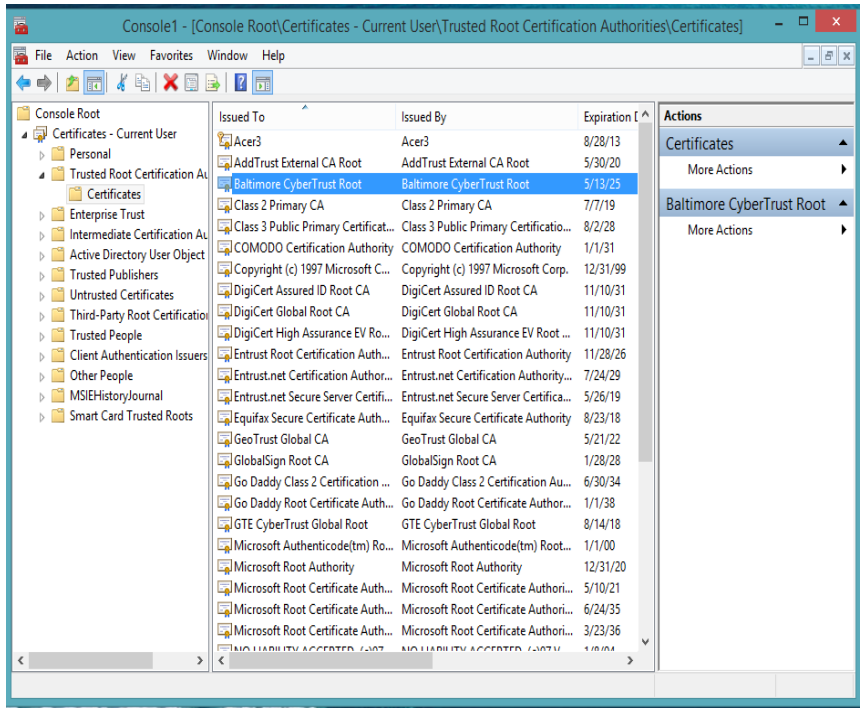
Certificate Authority (CA)

- A trusted third party that verifies and certifies the authenticity of the subject and the public key
- Issues Certificate
- Commercial/Public CAs
  - DigiCert, GlobalSign, Symantec, Comodo
- Private CAs
  - Used in an intranet environment
- Computers store a list of Trusted CA on the computer's Certificate Store. (Windows already has a list of CAs pre-installed on its certificate store)
- A **Certificate Store** is a secured storage on a computing device or media.
- Certificates must be issued by one of the list of Trusted CA in order to be trusted. (ie the public key in the certificate maps to the subject)

Certificate Search

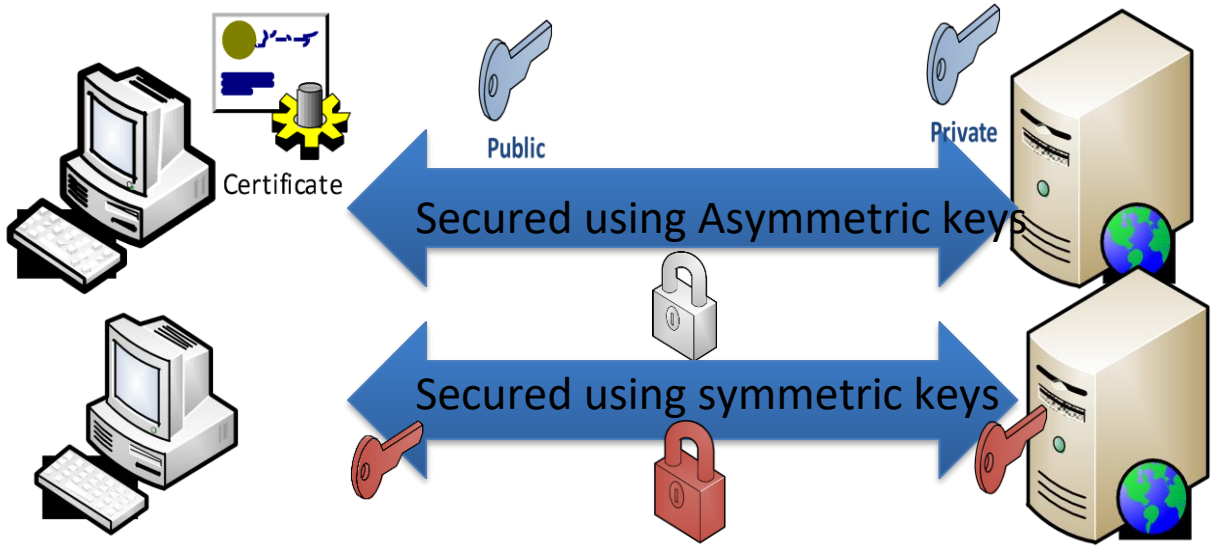
https://crt.sh/

Windows Certificate Store



SSL/TLS - Secure Socket Layer

- SSL/TLS is the de facto standard in protecting transmission on the Internet.
- TLS is the new name for SSL. For simplicity, we shall refer to it as SSL
- Client uses a public key from the server's certificate to initiate a encrypted session that exchange a shared secret key
  - The server's certificate must be issued by a trusted CAs recognized by the client computer
- This shared secret key is for subsequent encrypted sessions using symmetric encryption/decryption

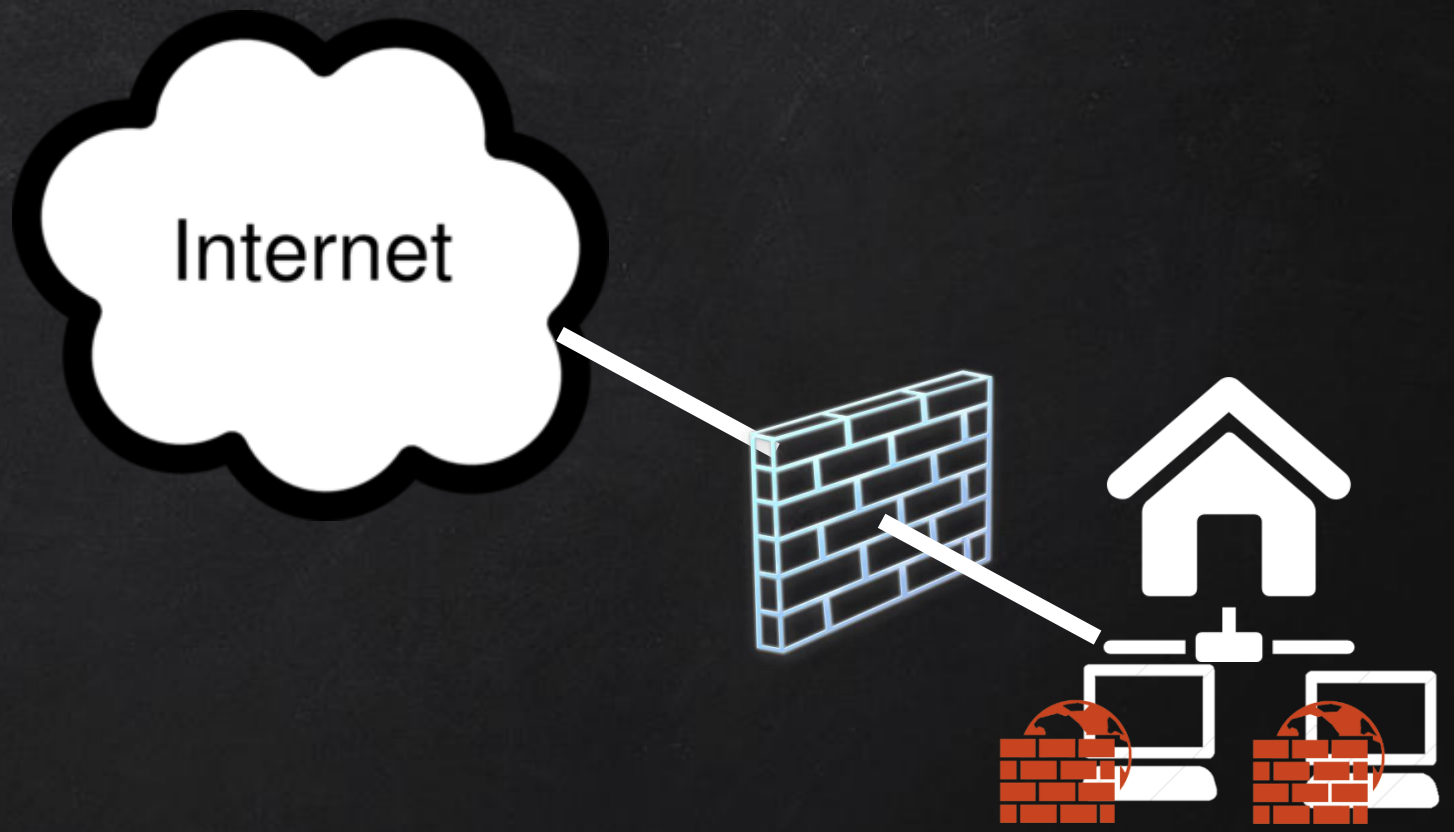


Unauthorised Access on the Network

- **Firewall**

– prevents unauthorised access

- Physical network device that is located between a public and a private network
- Software that runs on a computer.



–Monitors the traffic on the network

- identifies the source and type of application trying to gain access to
- Based on the rules configure, either block or allow access

Firewall

Packet filters

- Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules
- Packet filtering is fairly effective and transparent to users

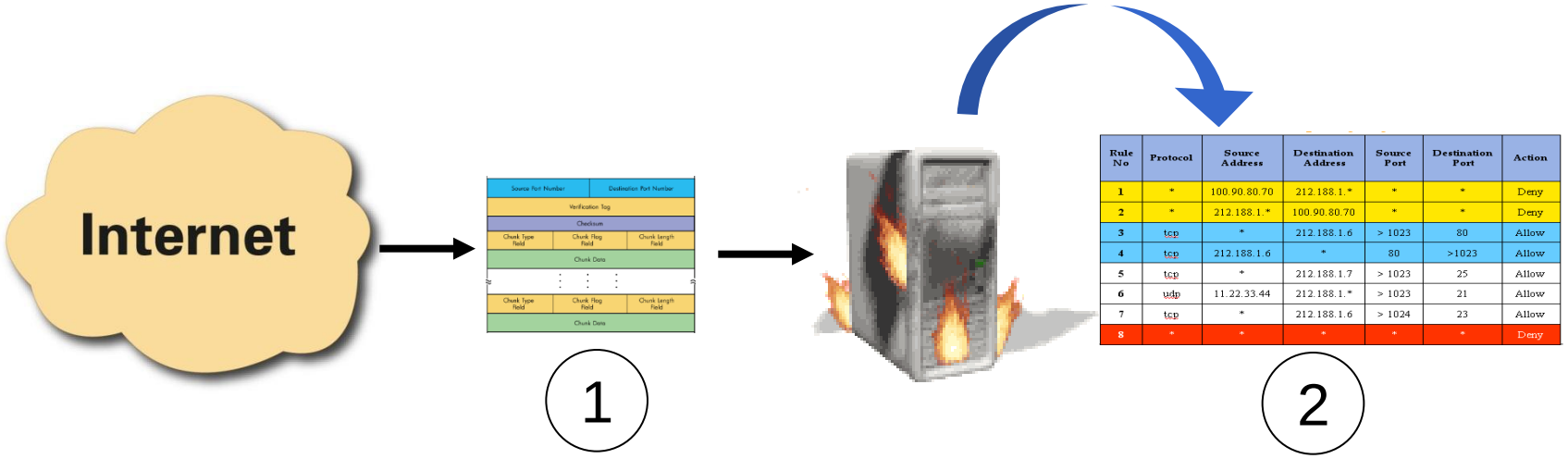
Packet Filtering

Location of the Packet Filter

- The packet filter can be placed at one of two places or both:
  - at the *network-level* (router-based)
  - at the *host-level* (host-based)

6.3 Packet Filtering

How packet filters are work (default-deny)



Rule No	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	*	100.90.80.70	212.188.1.*	*	*	Deny
2	*	212.188.1.*	100.90.80.70	*	*	Deny
3	tcp	*	212.188.1.6	> 1023	80	Allow
4	tcp	212.188.1.6	*	80	>1023	Allow
5	tcp	*	212.188.1.7	> 1023	25	Allow
6	udp	11.22.33.44	212.188.1.*	> 1023	21	Allow
7	tcp	*	212.188.1.6	> 1024	23	Allow
8	*	*	*	*	*	Deny

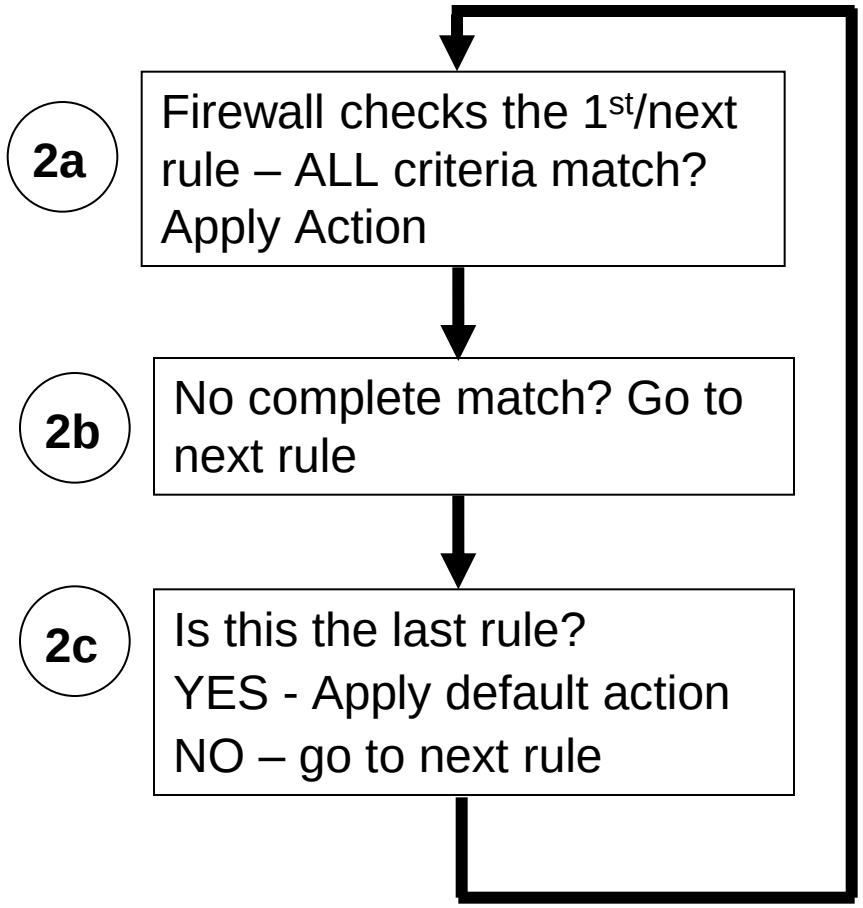
Packet meets firewall

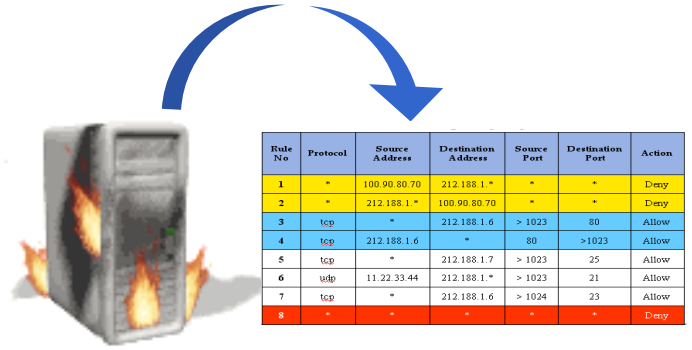
Firewall checks the packet against rules and decides if packet should be allowed thru

See next slide on how the decision is made

6.3 Packet Filtering

How the packet filter decides if packet is to be allowed through

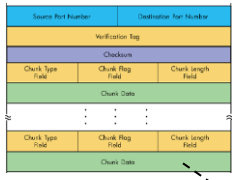




Rule No	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	*	100.90.80.70	212.188.1.*	*	*	Deny
2	*	212.188.1.*	100.90.80.70	*	*	Deny
3	tcp	*	212.188.1.6	> 1023	80	Allow
4	tcp	212.188.1.6	*	80	>1023	Allow
5	tcp	*	212.188.1.7	> 1023	25	Allow
6	udp	11.22.33.44	212.188.1.*	> 1023	21	Allow
7	tcp	*	212.188.1.6	> 1024	23	Allow
8	*	*	*	*	*	Deny

6.3 Packet Filtering

How the packet filter decides if packet is to be allowed through



Rule No	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	*	100.90.80.70	212.188.1.*	*	*	Deny
2	*	212.188.1.*	100.90.80.70	*	*	Deny
3	tcp	*	212.188.1.6	> 1023	80	Allow
4	tcp	212.188.1.6	*	80	>1023	Allow
5	tcp	*	212.188.1.7	> 1023	25	Allow
6	udp	11.22.33.44	212.188.1.*	> 1023	21	Allow
7	tcp	*	212.188.1.6	> 1024	23	Allow
8	*	*	*	*	*	Deny

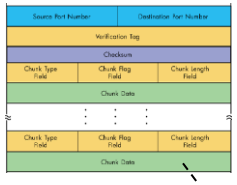
All fields in match those in rule 2?

YES – **Deny** packet, wait for next packet

NO – go to rule 3

6.3 Packet Filtering

How the packet filter decides if packet is to be allowed through



Rule No	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	*	100.90.80.70	212.188.1.*	*	*	Deny
2	*	212.188.1.*	100.90.80.70	*	*	Deny
3	tcp	*	212.188.1.6	> 1023	80	Allow
4	tcp	212.188.1.6	*	80	>1023	Allow
5	tcp	*	212.188.1.7	> 1023	25	Allow
6	udp	11.22.33.44	212.188.1.*	> 1023	21	Allow
7	tcp	*	212.188.1.6	> 1024	23	Allow
8	*	*	*	*	*	Deny

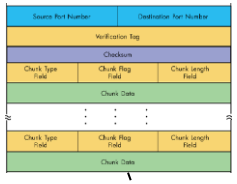
All fields in match those in rule 3?

YES – **Allow** packet, wait for next packet

NO – go to rule 4

6.3 Packet Filtering

How the packet filter decides if packet is to be allowed through



Rule No	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
1	*	100.90.80.70	212.188.1.*	*	*	Deny
2	*	212.188.1.*	100.90.80.70	*	*	Deny
3	tcp	*	212.188.1.6	> 1023	80	Allow
4	tcp	212.188.1.6	*	80	>1023	Allow
5	tcp	*	212.188.1.7	> 1023	25	Allow
6	udp	11.22.33.44	212.188.1.*	> 1023	21	Allow
7	tcp	*	212.188.1.6	> 1024	23	Allow
8	*	*	*	*	*	Deny

Since no rules match, apply the default rule

Firewall cannot detect and prevent

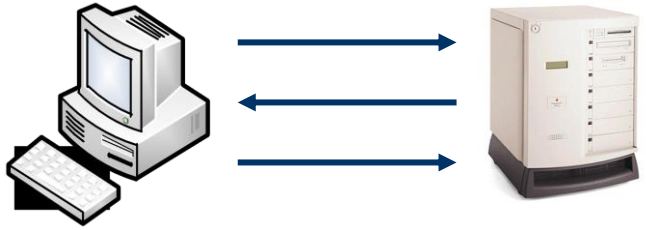
(Distributed) Denial of Service Attacks

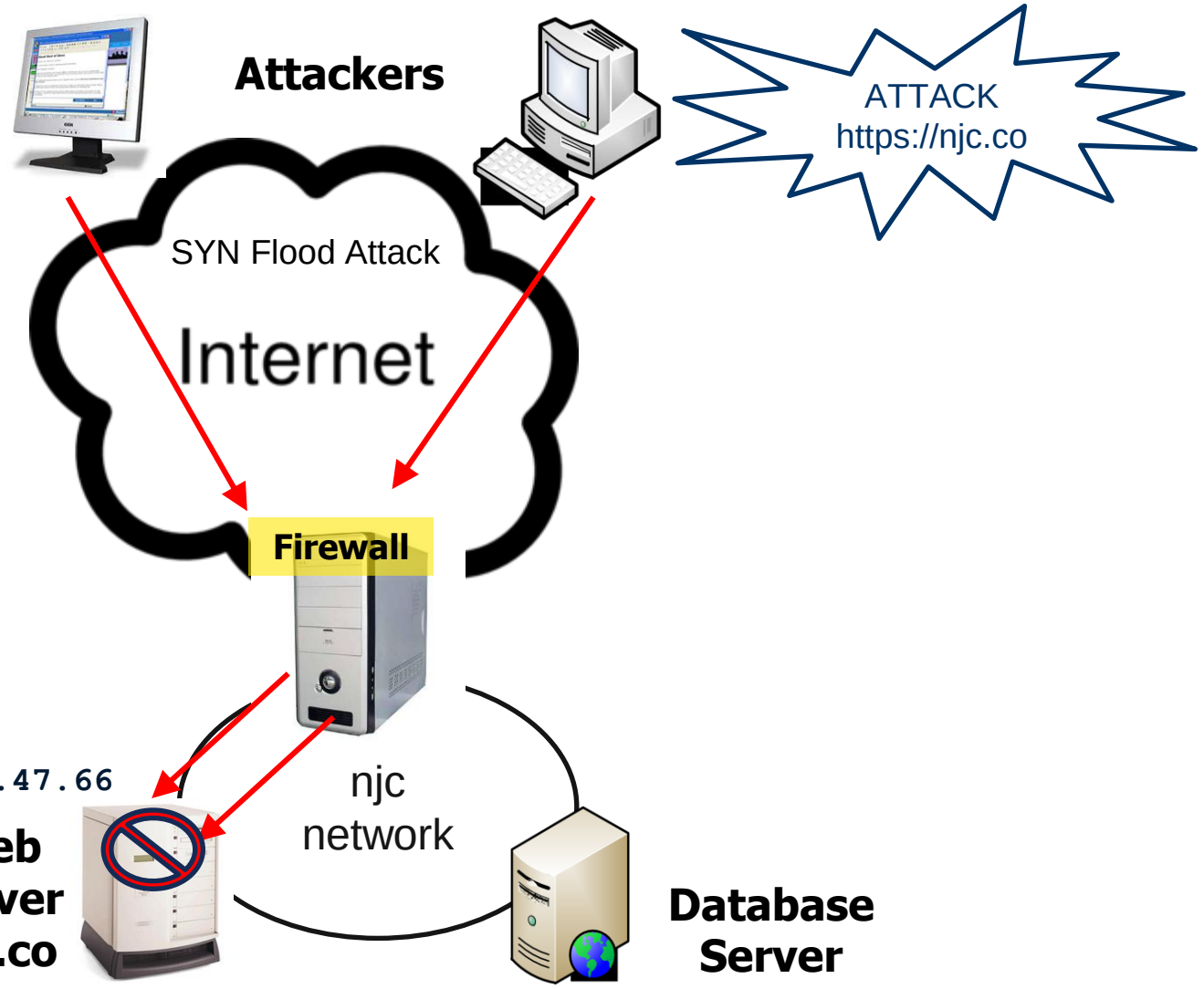
- - Overwhelm a server by flooding it with fake requests

Distributed Denial of Service Attack

Vulnerability

TCP 3-way Handshake





Intrusion Detection System (IDS)
vs
Intrusion Prevention Systems (IPS)

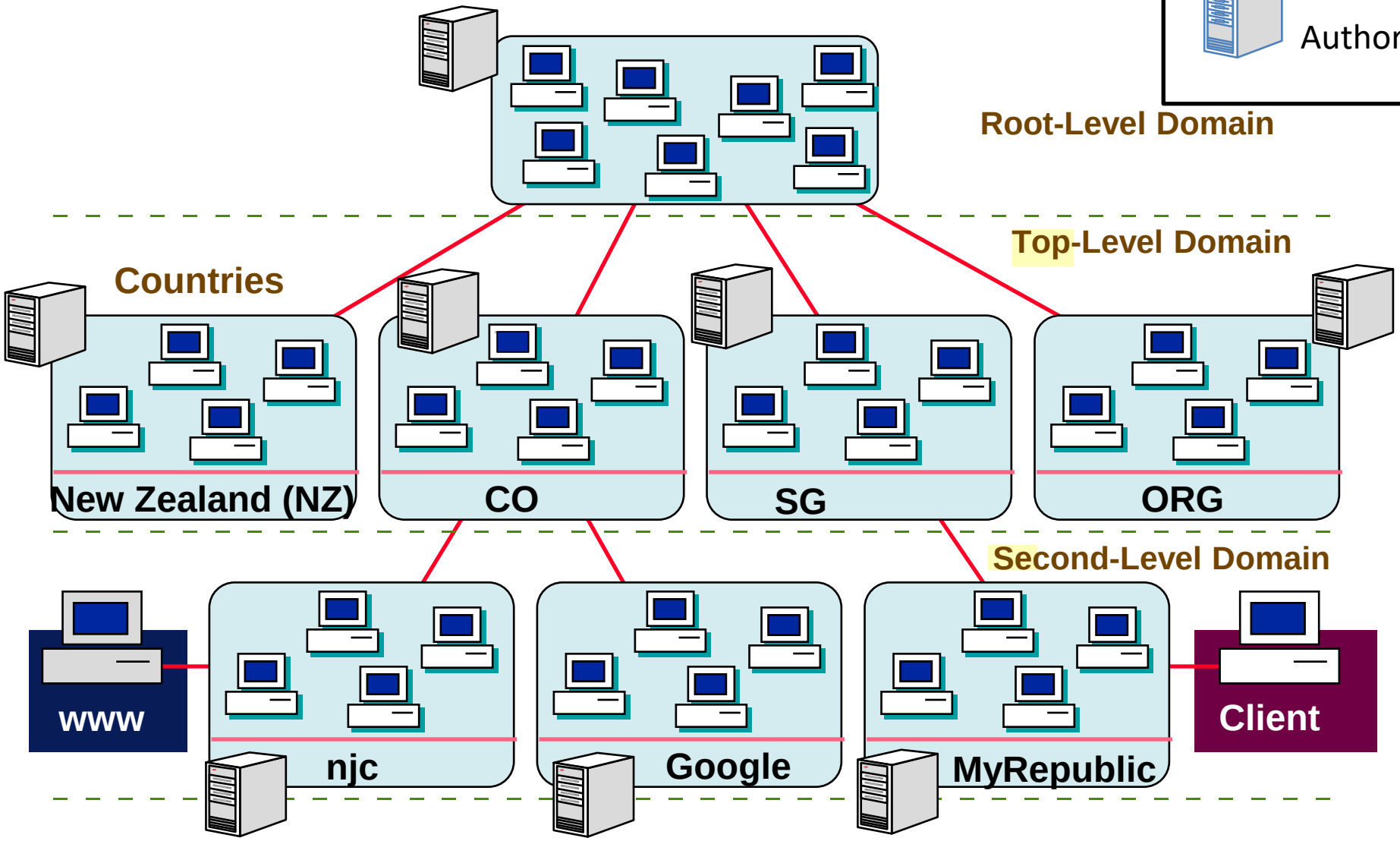
- Scan for patterns in the incoming packets
- IDS is passive
  - Only detects and send notifications
    - To prevent False Positives
  - Logs intrusions detected

- IPS is pro-active
  - Detects and Blocks
  - Logs intrusions detected

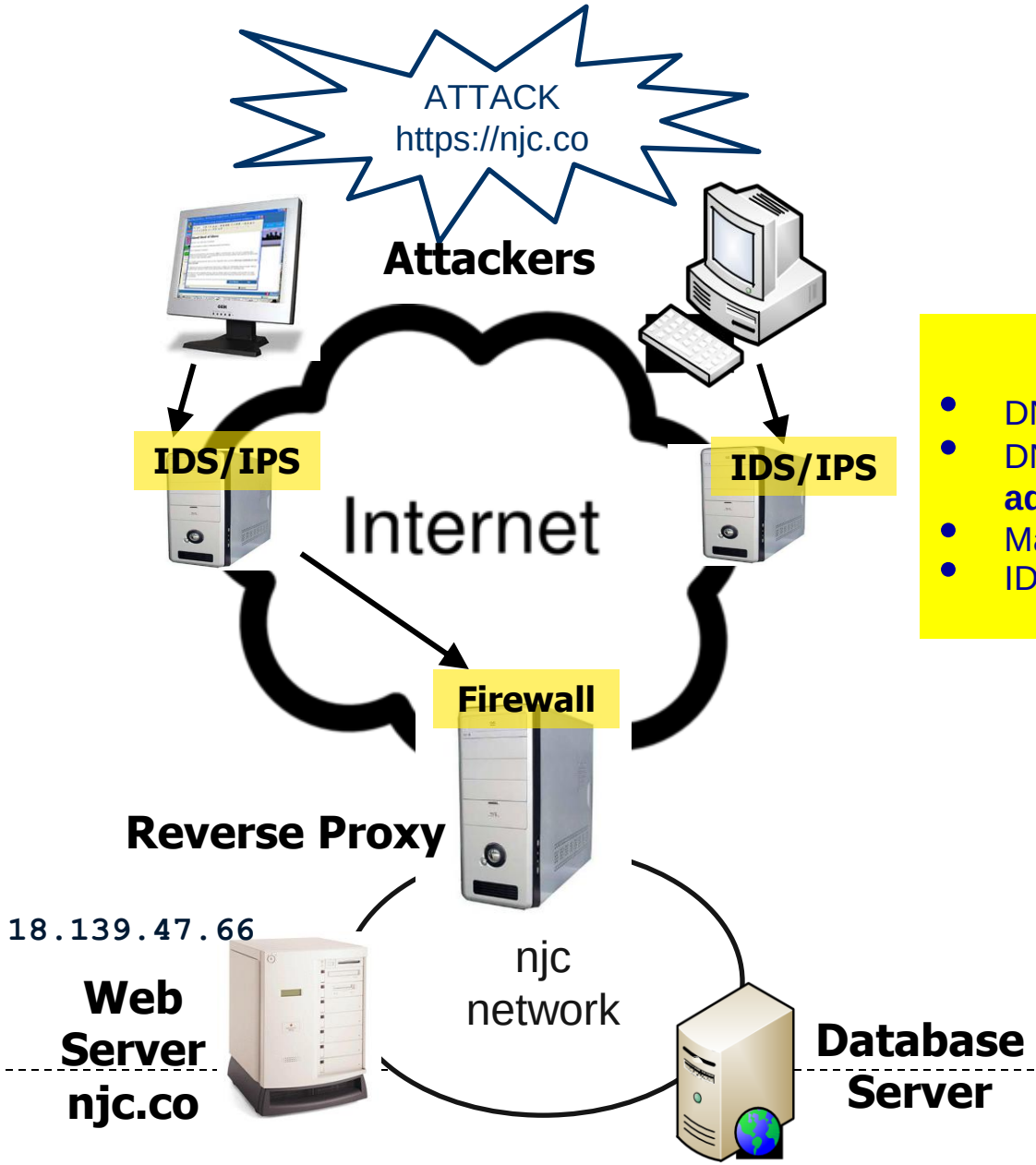
The Domain Name Service (DNS)

- To locate a resource on the Internet , we use a URL
  - https://njc.co/login which consists of the domain name and the resource
  - The domain name has to be resolved into an IP Address in order for the data packets to reach its destination. i.e njc.co must be resolved into 18 . 139 . 47 . 66
  - This DNS resolution is provided by DNS Servers on the Internet (by ISP)

Domain Name Space



Example : CloudFlare IDS/IPS



Reverse Proxy

- DNS will not resolve njc.co to `18.139.47.66`
- DNS will distribute all requests to njc.co to a **range of IP addresses** of CloudFlare's IDS/IPS servers
- Malicious traffic will be absorbed by the IDS/IPS
- IDS/IPS will forward only clean traffic to `18.139.47.66`