INF1001: Introduction to Computing

Part B

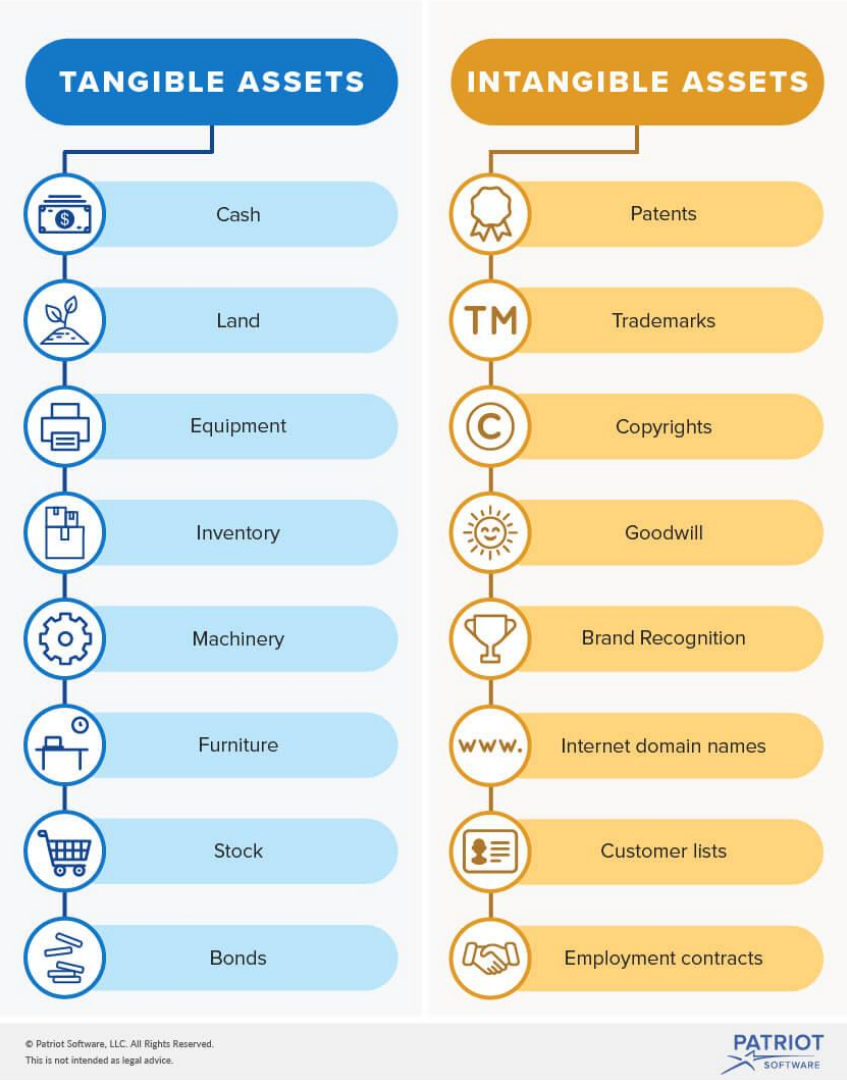
L4: Security

Aug 2023

Outline

- CIA Triangle
  - Confidentiality, Integrity & Availability
- Types of Attacks
  - Malwares, Botnets, DOS
- Protection
  - Authentication, Secured Connection, Encryption

Information as Assets



- **Physical assets**
  - Tangible
  - Less scalable
  - Incremental cost to produce
  - Transported via supply chain

VS

- **Information assets**
  - Intangible
  - Highly Scalable
  - Increasingly valuable and cost varied
  - Instant delivery

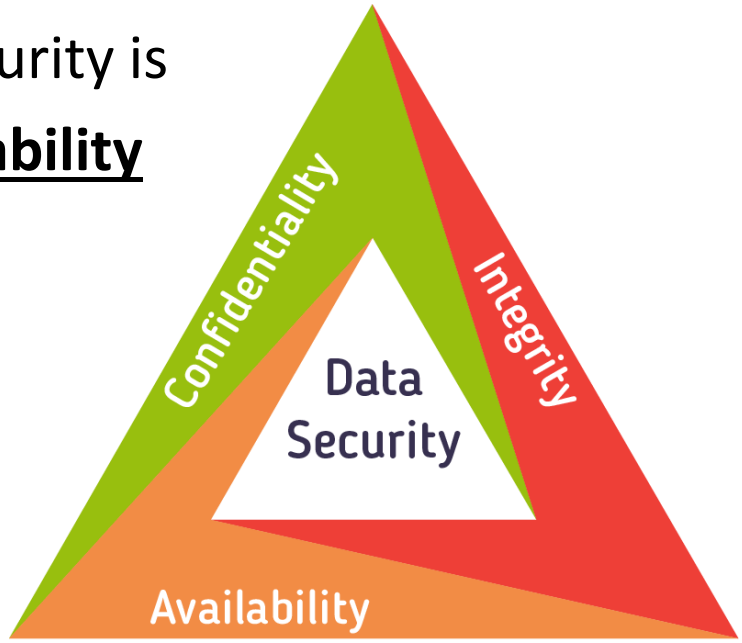
CIA Triangle/Triad

- The fundamental of Information Security is **Confidentiality**, **Integrity**, and **Availability**

  - **Confidentiality:** Information is only disclosed to those with the rights to know

  - **Integrity:** Information is correct and not manipulated in any way

  - **Availability:** Information is accessible and usable at all time.



integrity - Who is the creator of the CIA triad? - Information Security Stack Exchange

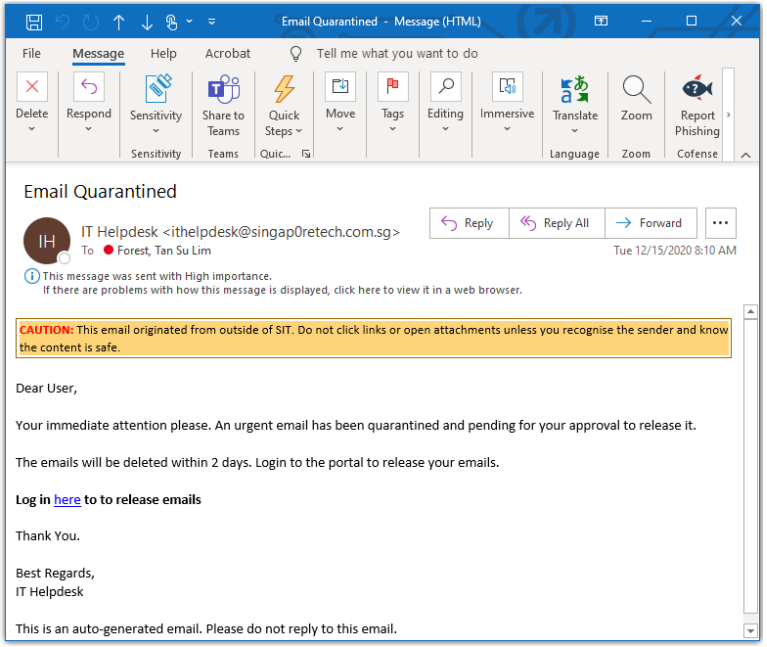
Types of Attacks

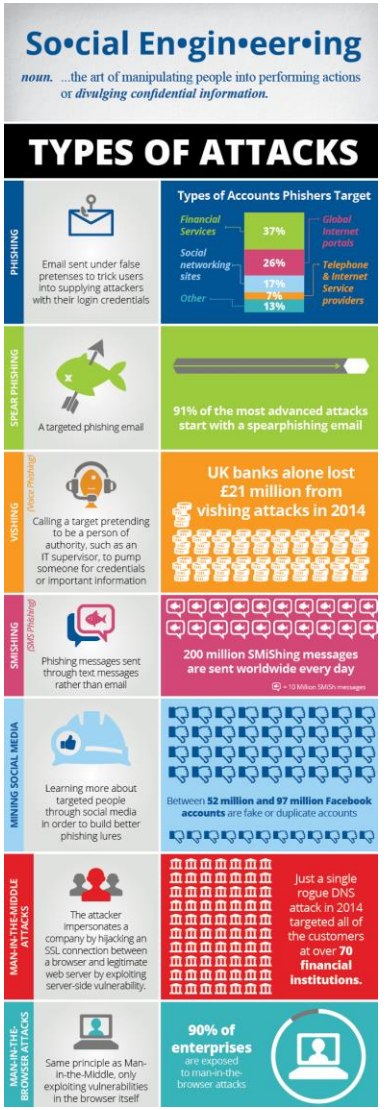
- Social Engineering
  - Phishing, Spear Phishing, Vishing, Smishing, Mining Social Media, Man-In-The-Middle Attack, Man-In-The-Browser Attack
- Malware
  - Virus, Worm, Trojan Horse, Spyware
- Denial Of Service (DOS)
- Botnets
- Spam

Social Engineering

- The art of manipulating people into performing actions or *divulging confidential information*

- Types of Attacks:
  - Phishing
  - Spear Phishing
  - Vishing
  - Smishing
  - Mining Social Media
  - Man-In-The-Middle Attack
  - Man-In-The-Browser Attack





- Crimes rise 11.6% in first half of 2020, driven by online scams preying on Covid-19 'fear, sense of uncertainty' - TODAY (todayonline.com)
- Crimes reported in S'pore rose 6.5% in 2020, fuelled by 65% jump in scam cases with over S$200m lost - TODAY (todayonline.com)
- $82 million lost through top 10 scams in first half of 2020, double the amount from a year ago, Courts & Crime News & Top Stories - The Straits Times

Social Engineering

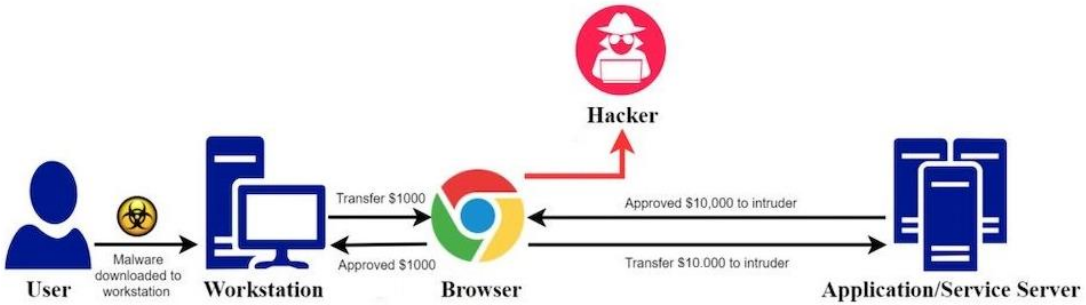
- The art of manipulating people into performing actions or *divulging confidential information.*

Social Engineering

- The art of manipulating people into performing actions or *divulging confidential information.*

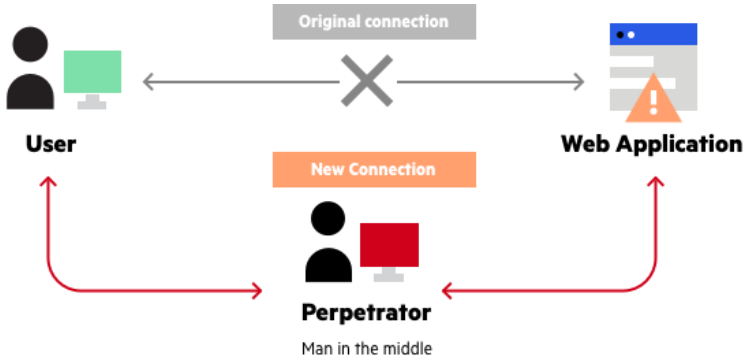
MAN-IN-THE-BROWSER ATTACKS

Same principle as Man-in-the-Middle, only exploiting vulnerabilities in the browser itself



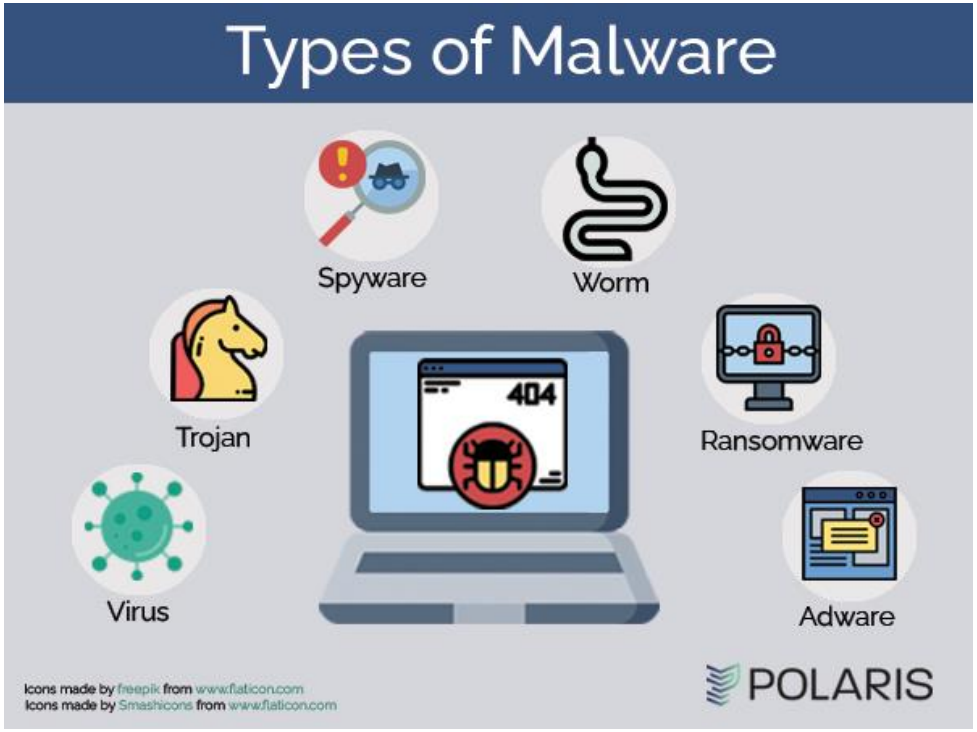
MAN-IN-THE-MIDDLE ATTACKS

The attacker impersonates a company by hijacking an SSL connection between a browser and legitimate web server by exploiting server-side vulnerability.



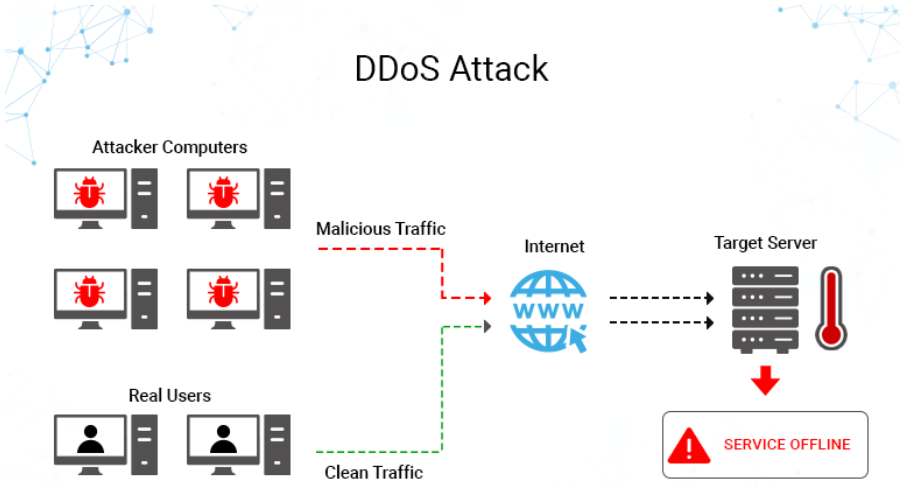
Malware - Malicious Software

- **Virus**: infects a host computer and spreads embed itself within another program or file
- **Worm**: Autonomous program that transfers itself through a network, taking up residence in computers and forwarding copies of itself to other computers
- **Trojan**: Program that enters a computer system disguised as a desirable program with harmful effects
- **Spyware**: Collects information about activities on computer and reports back to instigator of attack
- **Adware**: A form of malware that hides on your device and serves you advertisements
- **Ransomware**: Encrypts a victim's files and demands a ransom from the victim to restore access to the data upon payment



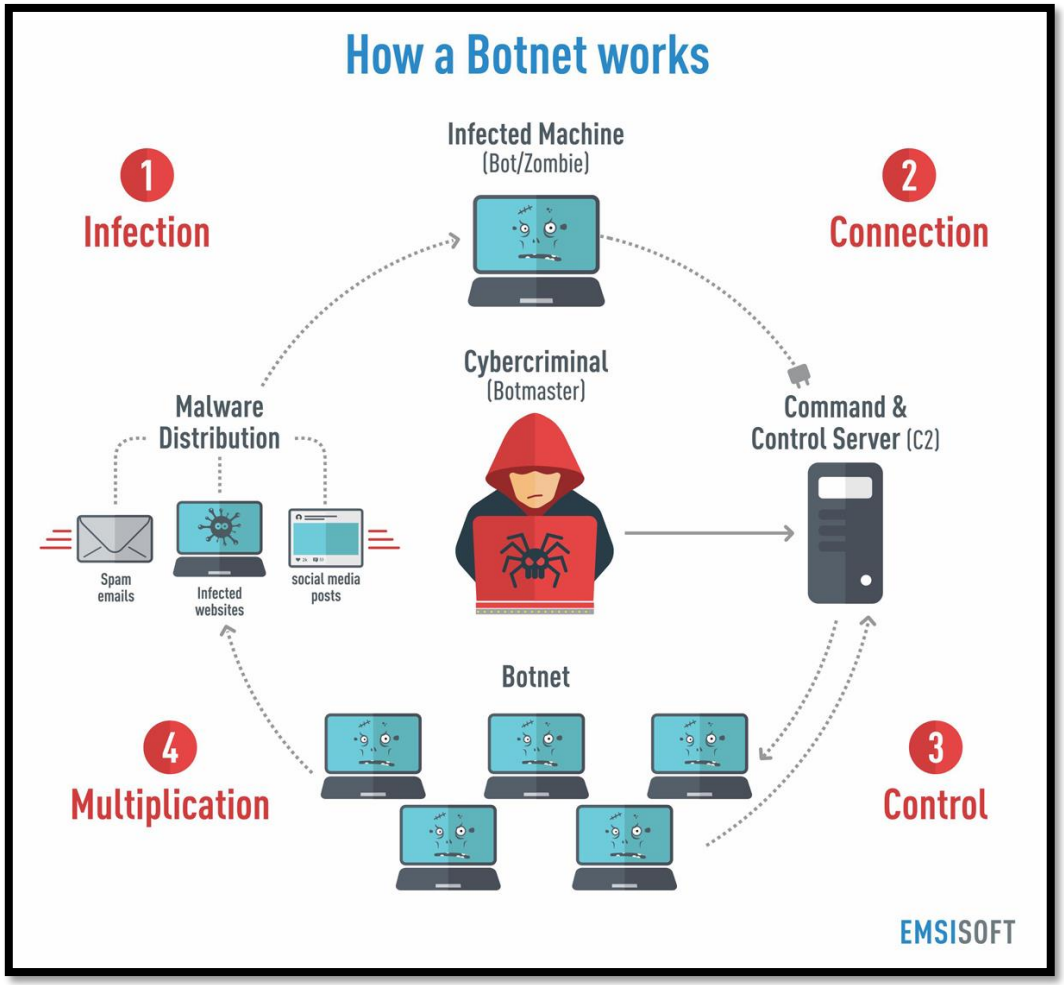
Denial of Service (DOS)

- Process of **overloading** a computer with messages
  - Software planted on unsuspecting computers to generate messages when signal is given
- **DDOS** – Distributed Denial of Service
  - Multiple systems flood the bandwidth or resources of a targeted system, usually compromised machines



https://www.straitstimes.com/tech/starhub-cyber-attacks-that-caused-broadband-outages-came-from-customers-infected-machines, Oct 2016

Botnets



- A common payload is to enable the infected computer to be remotely controlled by the worm/Trojan author
- Creation of a “zombie" computer
- **Botnet** - Large network (hundreds to millions) of compromised computers that communicate to commit DDOS, spam, phishing, etc.

Spam

- Abundance of unwanted messages

Quality Medicine Available C7 - The most complete Pha
Viagra Professional as low as $3.84 - Visit our new or
制-造-型-企-业-车-间 - 管-理-技-能-高-级-训-练 - GB2312?B
Re[13]: - Hot selling meds at cheeap All countriess shiipin
Our store is your cureall! - My Canadian Pharmacy We
We offer a variety of different licenses and discounts
Effortless Discount Offerings xh - Check Out our new
(no subject) -
We will help you get laid - Hey there. Just came across t
Lively Benefits of Creativity - When it comes to corpora
FW:hope you didn't mind - usasia , lcnd the liisi or ype b
RE: What's new out there? - tv-channel may dokeyromp
Looking to ReFi or a Home Equity Loan? - isn't some
We cure any desease! - My Canadian Pharmacy We shi
Unlimited Systemworks Downloads, get your 70% di
cheap oem soft shipping //orldwide - TOP 10 NEW TIT

Hackers

- Person who seeks and exploits weaknesses in a computer system or network ***without authorization*** for fun, profit or social causes

Black hat hackers: criminals who break into computer networks with malicious intent

White hat hackers: security experts who use their skills to identify vulnerabilities in computer systems and networks

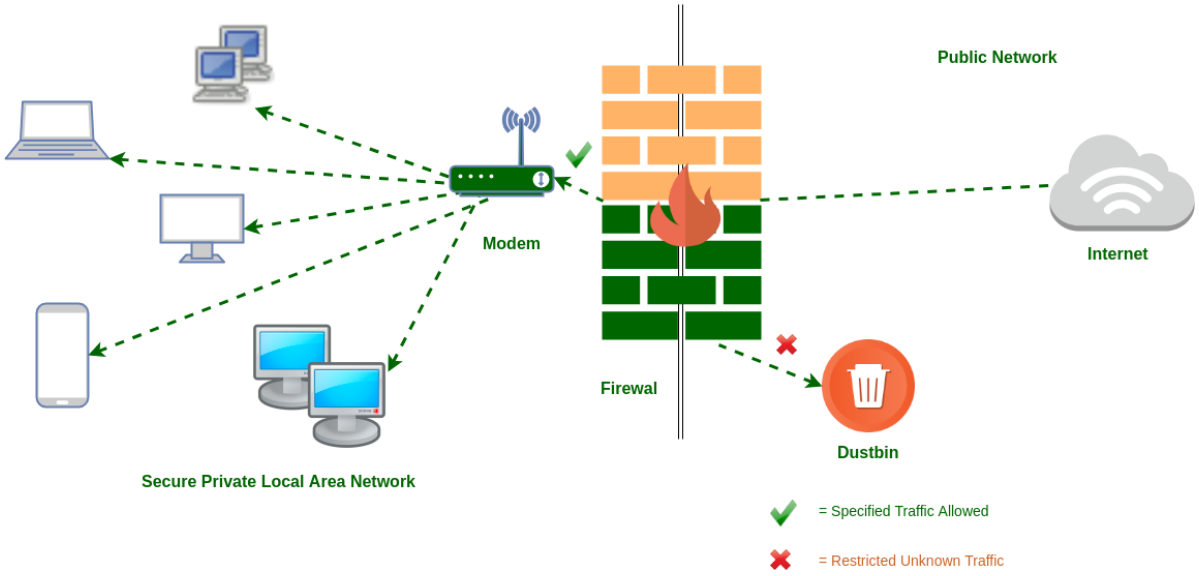
Grey hat hackers: blend of both black hat and white hat activities

Protection techniques

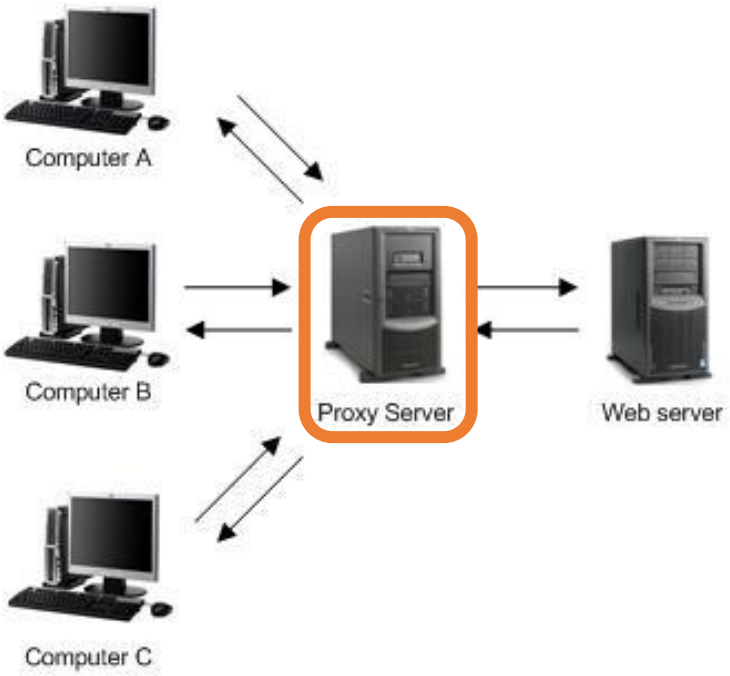
- Firewall
- Proxy Server
- Network Auditing Software
- Anti-Virus
- Secured Connection – SSL
- Authentication
- Cryptography

Firewall

- Installed at company's intranet to filter messages passing in and out
  - Acts like a security guard at the gate (usually a physical hardware)
  - Typically filters IP addresses, ports, protocols, etc.



Proxy Server



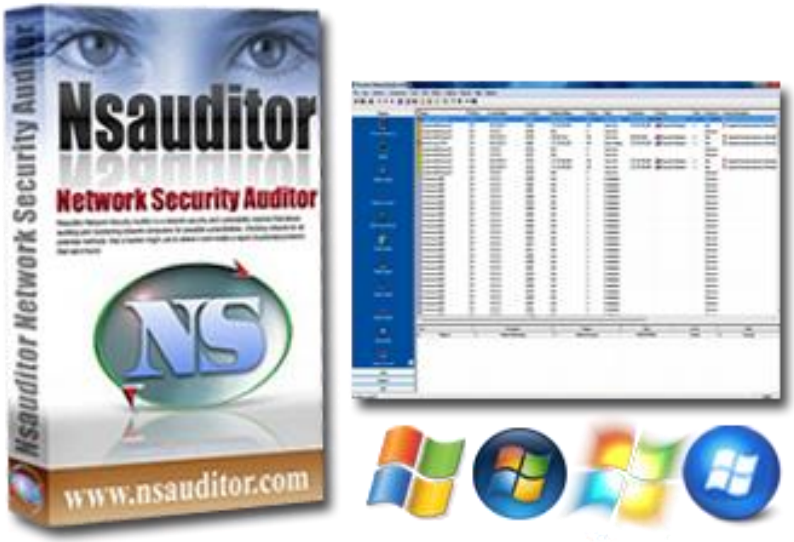
Difference Between Firewall and Proxy Server

	FIREWALL	PROXY SERVER
Basic	Monitors and filters the incoming and outgoing traffic in a local network.	Establishes the communication between the external client and the server.
Filters	IP packets	Client-side requests for the connection.
Generated overhead	More	Less
Involves	Network and Transport layer data.	Application layer data.

- Acts as an intermediary between client and server to shield client from adverse actions of the server.
- Proxy server deals with the **application-level** traffic and filter the requests coming from the unknown client
  - Server has no way of learning about intranet's internal features
  - Filters all messages sent from server to client

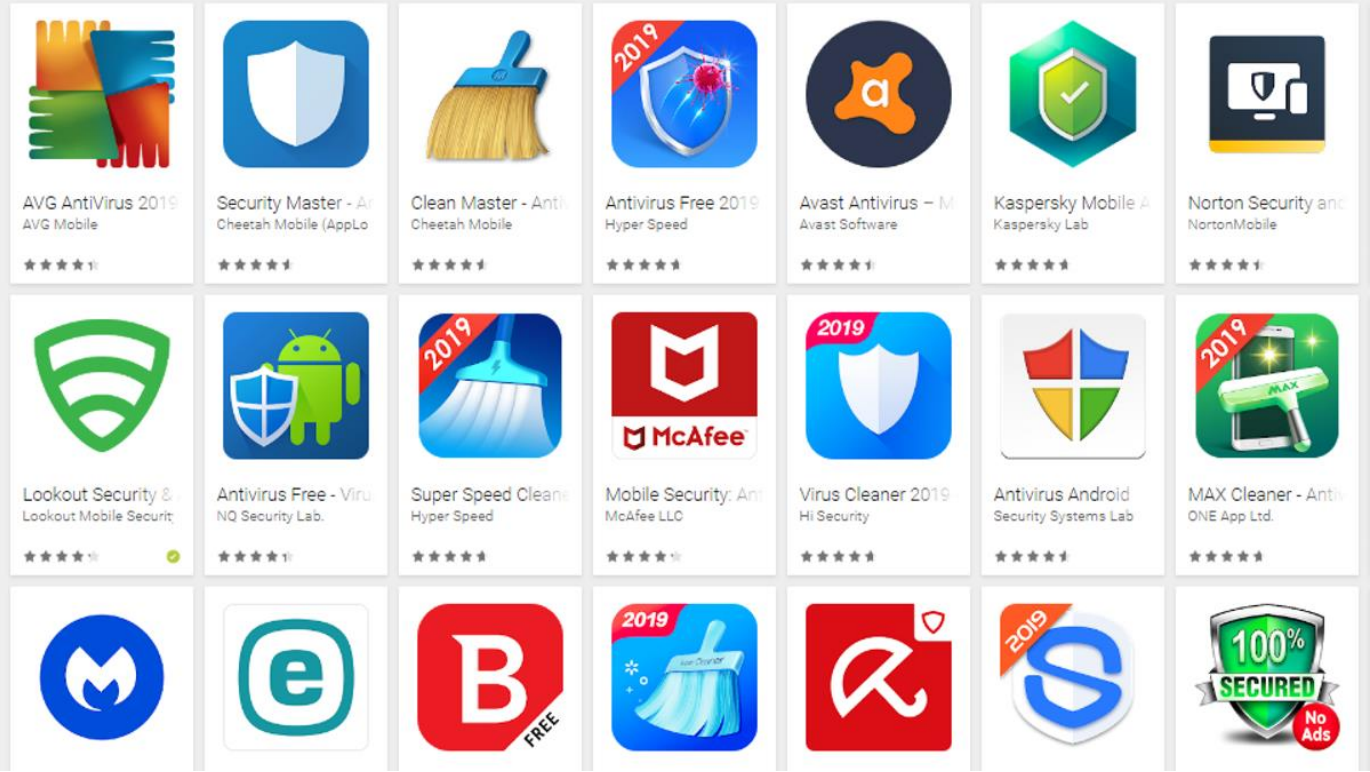
Network Auditing Software

- Software used to **determine weaknesses/ vulnerabilities** in the network or systems
  - Can be used for good by proactively identifying and fixing vulnerabilities
  - Can be abused by attackers to probe for vulnerabilities before exploiting them



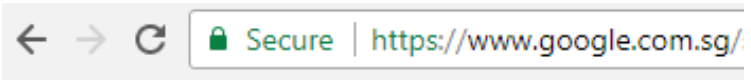
Anti-Virus

- Detect and remove presence of viruses and infections

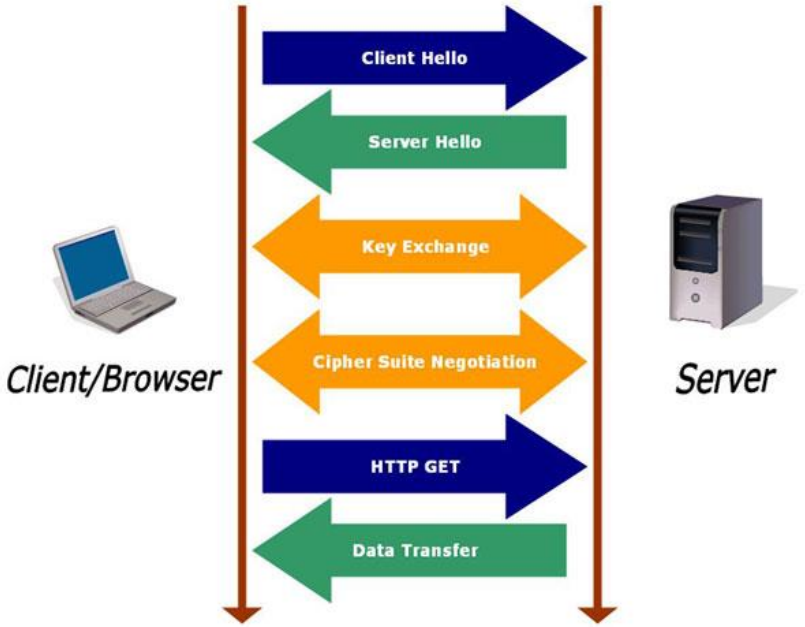


Secured Connection

- Secured version of applications
  - FTPS: File Transfer Protocol Secure
  - HTTPS: Hypertext Transfer Protocol Secure



- Use Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
  - Internet security protocol which encrypt the connection between your web browser and a website



What is SSL/TLS? [2:16]

https://www.youtube.com/watch?v=345hgmT4NAo

Authentication

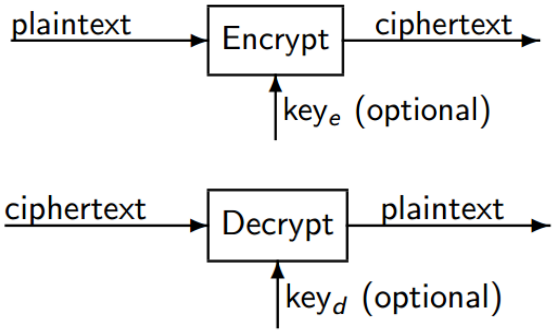
- Commonly Uses Passwords

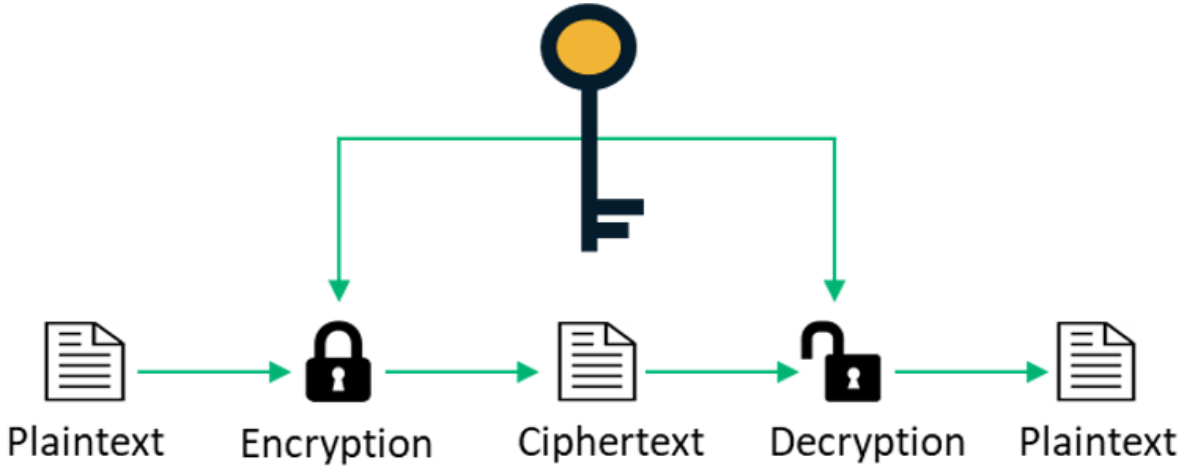
- Biometric information
  - Fingerprint scanning

- 2FA (Two Factor Authorization) using (Digital) Tokens
  - Your password + one-time password

Cryptography

- Science of 'secret' writing
  - Render a message less useful/meaningful to any eavesdropper
- Process of **encryption**
  - Message (**plaintext**) is encrypted before it is sent
- Process of **decryption**
  - **Ciphertext** is decoded back when it is received





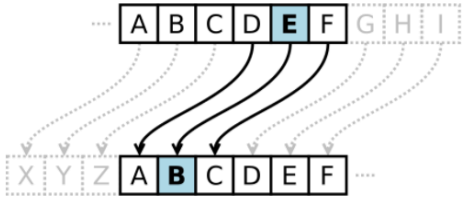
Encryption algorithms

- **Symmetric encryption:**
  - Use **same** secret key to encrypt and decrypt
    - Sender & receiver knows the same key
  - Challenge is how to transmit the same secret key?
  - E.g., Caesar cipher, Block cipher, DES, AES

- **Asymmetric encryption:**
  - Use **different** secret key to encrypt and decrypt
    - Sender & receiver knows different keys
  - E.g., RSA

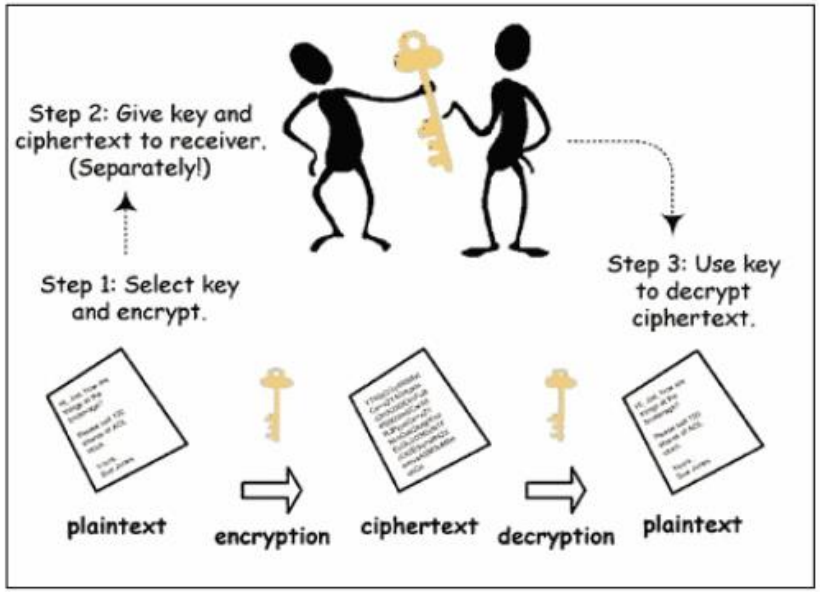
(Sym Encrypt) Caesar Cipher

- Also called **Shift Cipher**
- Shifting <u>each</u> character in message to another character some <u>fixed distance</u> farther along the alphabet



Shift left 3

```
Plaintext:
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext:
QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```



(Sym Encrypt) Block Cipher

- Unlike stream cipher which encrypts a character at a time, block cipher encrypts a block of text at a time
- A block of plaintext gets encoded into a block of ciphertext
- Destroys structure of plaintext and make decryption more difficult
- Examples: Hill Cipher & DES encryption

(Sym Encrypt) Hill Cipher Encryption

Want to encrypt the plain text message "short example" using keyword "hill"

1. Turn keyword into a matrix

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

The keyword written as a matrix.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

The key matrix.

A	B	C	D	E	F	G	H	I	J	K	L	…
0	1	2	3	4	5	6	7	8	9	10	11	

2. Convert plain text to matrices

$$\begin{pmatrix} s \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix}$$

The plain text "short example" split into column vectors.

$$\begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

The plain text converted into numeric column vectors.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(Sym Encrypt) Hill Cipher Encryption

$K=\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}$ The key matrix.

$\begin{pmatrix}18\\7\end{pmatrix}\begin{pmatrix}14\\17\end{pmatrix}\begin{pmatrix}19\\4\end{pmatrix}\begin{pmatrix}23\\0\end{pmatrix}\begin{pmatrix}12\\15\end{pmatrix}\begin{pmatrix}11\\4\end{pmatrix}$ The plain text converted into numeric column vectors.

In General:

To multiply an **m×n** matrix by an **n×p** matrix, the **n**s must be the same, and the result is an **m×p** matrix.

m × n × n × p → m × p

3. Matrix multiplication

[How to Multiply Matrices (mathsisfun.com)]

$$\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\begin{pmatrix}18\\7\end{pmatrix}=\begin{pmatrix}182\\275\end{pmatrix}$$

$$7\times 18+8\times 7=182$$
$$11\times 18+11\times 7=275$$

4. Modulo 26

[Modulo operation - Wikipedia]

$$\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\begin{pmatrix}18\\7\end{pmatrix}=\begin{pmatrix}182\\275\end{pmatrix} \xrightarrow{\text{mod } 26} \begin{pmatrix}0\\15\end{pmatrix}$$

$$\begin{pmatrix}18\\7\end{pmatrix}\begin{pmatrix}14\\17\end{pmatrix}\begin{pmatrix}19\\4\end{pmatrix}\begin{pmatrix}23\\0\end{pmatrix}\begin{pmatrix}12\\15\end{pmatrix}\begin{pmatrix}11\\4\end{pmatrix} \rightarrow \begin{pmatrix}0\\15\end{pmatrix}\begin{pmatrix}0\\3\end{pmatrix}\begin{pmatrix}9\\19\end{pmatrix}\begin{pmatrix}5\\19\end{pmatrix}\begin{pmatrix}22\\11\end{pmatrix}\begin{pmatrix}5\\9\end{pmatrix}$$

$$\begin{pmatrix}s\\h\end{pmatrix}\begin{pmatrix}o\\r\end{pmatrix}\begin{pmatrix}t\\e\end{pmatrix}\begin{pmatrix}x\\a\end{pmatrix}\begin{pmatrix}m\\p\end{pmatrix}\begin{pmatrix}l\\e\end{pmatrix} \rightarrow \begin{pmatrix}A\\P\end{pmatrix}\begin{pmatrix}A\\D\end{pmatrix}\begin{pmatrix}J\\T\end{pmatrix}\begin{pmatrix}F\\T\end{pmatrix}\begin{pmatrix}W\\L\end{pmatrix}\begin{pmatrix}F\\J\end{pmatrix}$$

"hill"

"Short example"  "APAD J TFTWLFJ"

(Sym Encrypt) Hill Cipher Decryption

To decrypt, we need to find the **inverse** Key (K^{-1}) matrix: Inverse of a Matrix (mathsisfun.com)

$$K^{-1} = det^{-1} adj(K)$$

(A) (B)

$$k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad K^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Note: **ad−bc** is called the determinant.

A 1 $determinant\ of\ Key \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

$$det = 7(11) - 8(11) = -11\ (mod\ 26) = 15$$

B $adj(K)\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} mod\ 26$

$$= \begin{bmatrix} \mathbf{11} & \mathbf{18} \\ \mathbf{15} & \mathbf{7} \end{bmatrix}$$

A 2 $det.det^{-1}(mod\ 26) = 1$

$$15.det^{-1}(mod\ 26) = 1$$

$$15 \times 7 = 105\ (mod\ 26) = 1$$

$$det^{-1} = 7$$

$$K^{-1} = 7.\begin{bmatrix} \mathbf{11} & \mathbf{18} \\ \mathbf{15} & \mathbf{7} \end{bmatrix} = \begin{bmatrix} 77 & 126 \\ 105 & 49 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

For decryption, you inverse the key matrix

$Decryption\ of\ ciphertext, \begin{bmatrix} 0 \\ 15 \end{bmatrix}$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}$$

Polygraphic Part 2 - Hill Ciphers Examples/Encryption/Decryption - YouTube

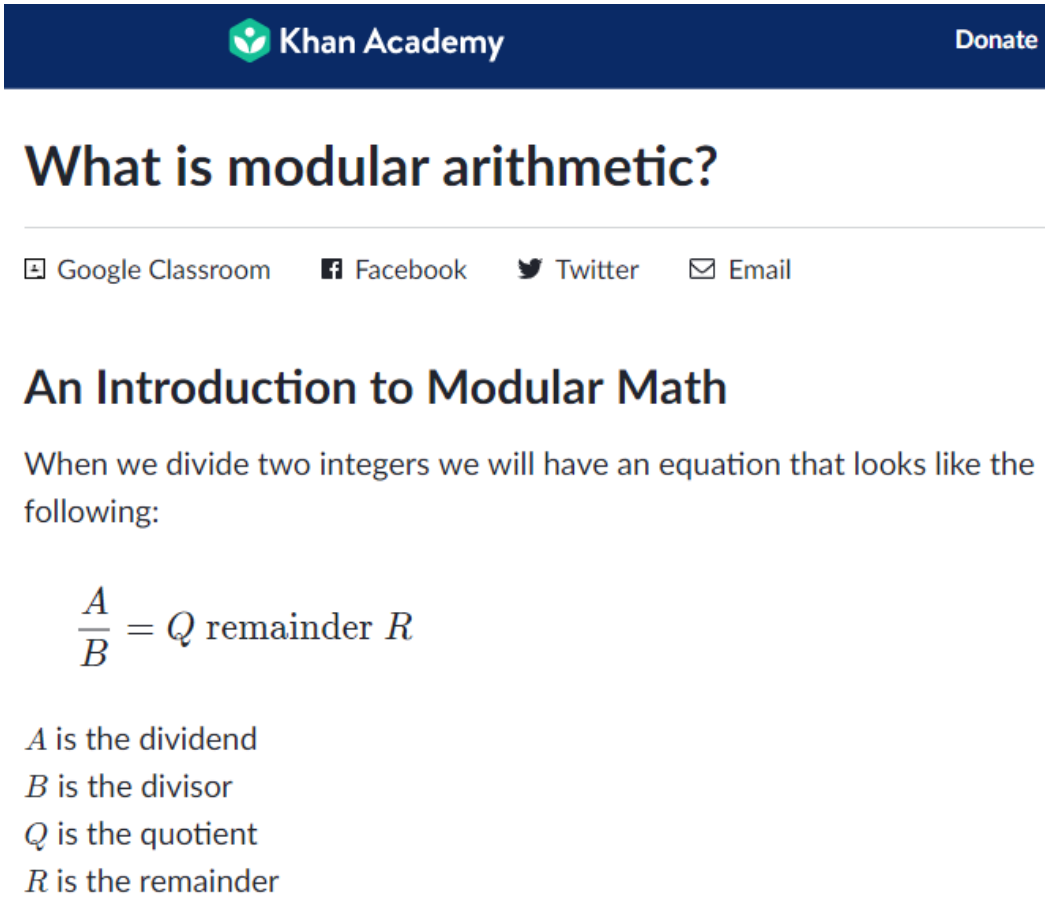
(Sym Encrypt) Hill Cypher Decryption – More reading

- For modulus arithmetic, refer to:

  https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic

- For Hill Cipher, refer to:

  http://crypto.interactive-maths.com/hill-cipher.html



Khan Academy Donate

What is modular arithmetic?

Google Classroom Facebook Twitter Email

An Introduction to Modular Math

When we divide two integers we will have an equation that looks like the following:

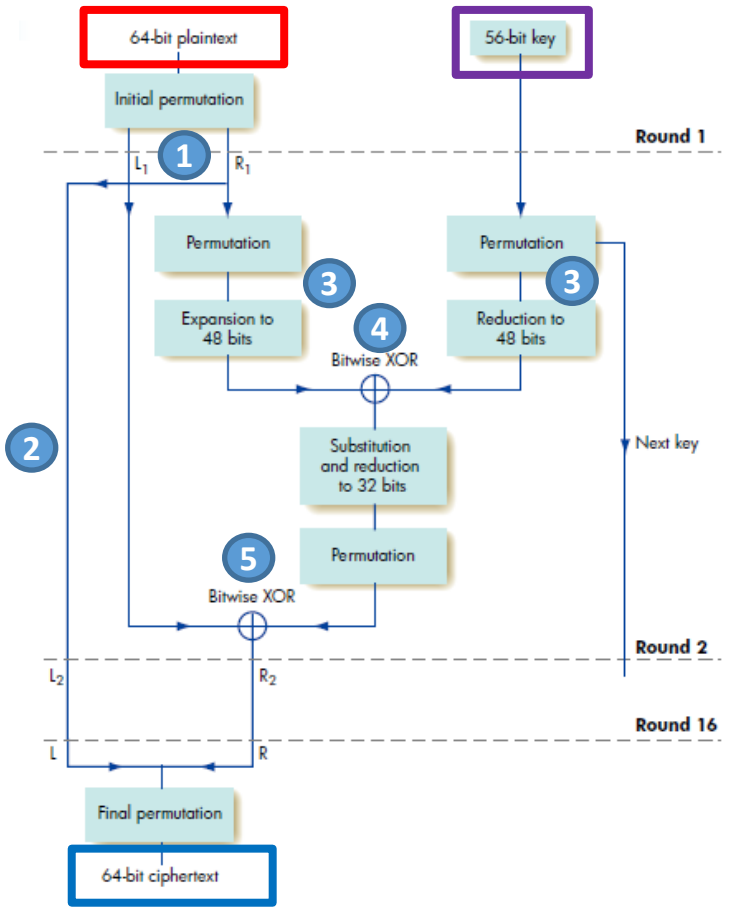
$$\frac{A}{B} = Q \text{ remainder } R$$

A is the dividend
B is the divisor
Q is the quotient
R is the remainder

(Sym Encrypt) DES

- Stands for **Data Encryption Standard**
- Block Cipher where blocks are 64 bits long, so 64 plain-text bits are processed at a time into 64 ciphertext bits.
- The key is 64-bit binary key
  - Actually only 56-bit is used, the other 8-bit is used for parity checks
  - Hence, **effective key length is 56-bit**
- Given same plaintext and same key, everyone using DES ends up with same ciphertext
- Same algorithm serves for decryption – reverse order

DES Encryption Algorithm



General Steps:

1. *Incoming 64-bit plaintext block is split into left half L_i and right half R_i*
   - *R_i is unchanged to become left half in next round*
2. *At the same time. R_i permuted, and expanded. Key is permuted and reduced*
3. *XOR R_i with Key*
4. *Resultant is then XOR with L_i. This becomes the next R_i*
5. *Altogether, algorithm goes through 16 rounds*

Data Encryption Standard (tutorialspoint.com)

Enhancements to DES

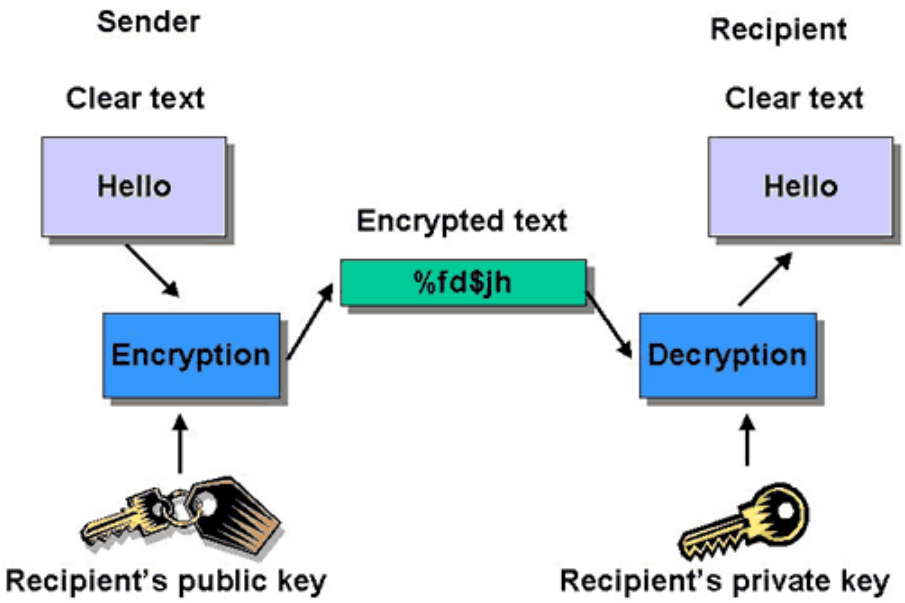
- With increased computing power, DES is easily broken:
  - 1976: DES approved as a standard
  - 1994: 1st experimental cryptanalysis of DES performed
  - 1997: DESCHALL Project breaks DES message for 1st time
  - 1999: DES key broken in 22 hours and 15 minutes

- Triple DES
  - Naïve approach requires two 56-bit keys
  - Runs DES three times: encode using key #1, decode using key #2 and encode using key #1 again

- AES (Advanced Encryption Standard)
  - Published in 2001 as FIPS (Federal Information Processing Standard) 197 standard
  - Key length: 128, 192 or even 256 bits

(Asym Encrypt) Public Key Systems

- Recipient has a pair of keys:
  - Public key – shared with public
  - Private key – only known by the recipient
- To send encrypted message, always encrypt using recipient's **public key**



(Asym Encrypt) RSA

- RSA = (Ron **Rivest**, Adi **Shamir** and Leonard **Adleman**)
- Success of RSA is because it is **extremely difficult** to **find the prime factors for n**, if n is a large number

SN	Actions	Remarks	Example
1	**Select** p and q	p and q are large prime numbers chosen randomly *But for illustration, in this slide, we deliberately choose small p and q.*	p = 3, q = 7
2	Compute n = p × q	n is also known as *modulus*	n = 3 × 7 = 21
3	Compute m = (p-1) × (q-1)	m is also known as *totient*	m = (3-1) × (7-1) = 2 × 6 = 12
4	**Select** e	e is chosen such that e and m has no common factors, i.e. gcd (e, m) = 1 or what is known as co-prime of m e is also known as *public exponent*	e = 5 because: • m = 12 (1 × 12 or 2 × 6 or 3 × 4) • e = 5 (1 × 5) • m and e have no common factors
5	Compute d	(d×e) mod m = 1 d is also known as *private exponent*	(d×5) mod 12 = 1 d = 5

e	d	e * d	(e * d) mod 12
5	1	5	5
5	2	10	10
5	3	15	3
5	4	20	8
5	5	25	1
5	6	30	6

Greatest Common Divisor (GCD) | Find GCD with Examples (byjus.com)

(Asym Encrypt) RSA

- The number pair (n, e) becomes **public** key
- The number d becomes **private** key
- p, q, e are chosen randomly
- n, m, d are relatively easy to compute

$n = p \times q$
$m = (p-1) \times (q-1)$
$(d \times e) \bmod m = 1$

- Let M = plaintext, C = Ciphertext

- Sender encrypt: $\mathbf{C = M^e \bmod n}$

- Recipient decrypt: $\mathbf{M = C^d \bmod n}$

(Asym Encrypt) RSA

- Following the previous example where the following was:
  - Chosen randomly: p = 3, q = 7, e = 5
  - Computed: n = 21, m = 12, d = 5
- Recall:
  - The number pair (n, e) becomes **public** key
  - The number d becomes **private** key
  - Sender encrypt: $C = M^e \bmod n$
  - Recipient decrypt: $M = C^d \bmod n$

Action	Plaintext	Ciphertext
Sender encrypts plaintext, M. Supposing M = 4	M = 4 ⇒	$C = M^e \bmod n$ $C = 4^5 \bmod 21$ $C = 1024 \bmod 21$ C = 16
Recipient decrypts ciphertext, C and gets back original plaintext, M = 4	⇐ $M = C^d \bmod n$ $M = 16^5 \bmod 21$ $M = 1{,}048{,}576 \bmod 21$ M = 4	C = 16

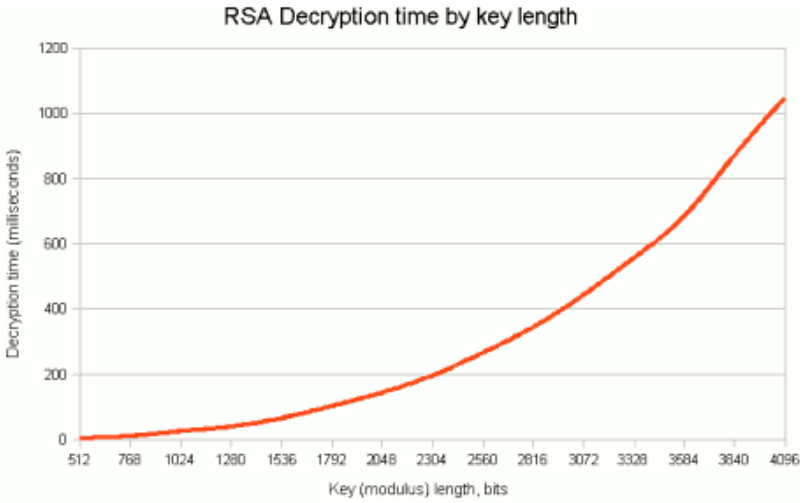
Beauty of RSA

- Attackers know the public key, i.e. the number pair (n, e) and the Ciphertext, C
- But can attackers reverse the plaintext, $M = C^d \bmod n$?
- Remember that attackers do not know d!
- Recall d is private key, known only to recipient
  - $(d \times e) \bmod m = 1$
- Attackers know e so can they guess what is d?
- They cannot because they don't know what is m!
- Can attackers guess what is m then?
  - Recall $m = (p-1) \times (q-1)$ and $n = p \times q$
- Recall attackers know n, so surely they can guess p and q?
  - E.g. if n = 21, surely attackers can easily find out p = 3 and q = 7, right?

Beauty of RSA

- Yes, attackers can easily guess p and q, if p and q are small prime numbers which results in a small n
  - Recall that n = 21 and since n = p × q, therefore p = 3 and q = 7, which can be easily guessed by attackers since p and q are small prime numbers
- But what if p and q are large prime numbers that results in a large n?
- E.g., what if n is 2059? What is p and q? Can you guess?

- While it is easy to calculate n given p and q, it is very difficult to do the reverse, i.e. to calculate p and q given n



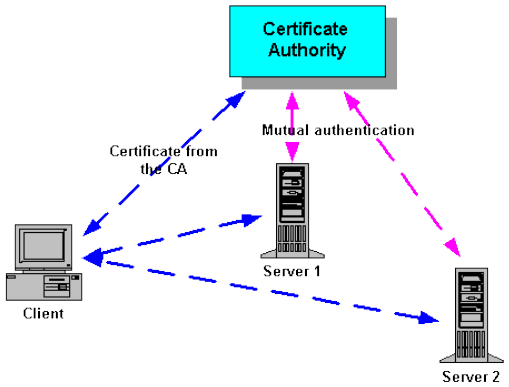
- Therefore, the success of RSA is because it is **extremely difficult** to **find the prime factors for n**, if n is a large number

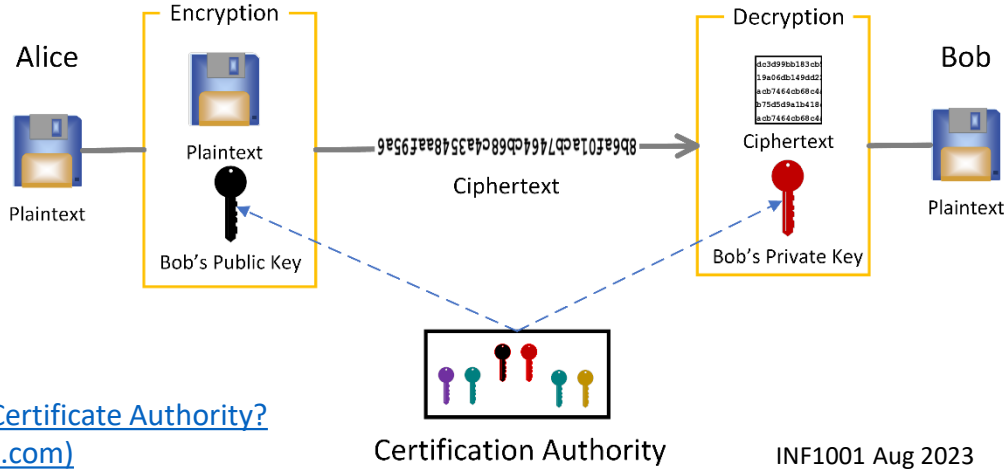
- RSA started with 1024-bit key, 2048-bit (smart card, Ransomware) to 4096-bit Transport Layer Security) as the most robust and most uncrackable (for now).

[What is RSA-4096 Ransomware & How to Protect Against It in 2021? (comparitech.com)]

(Asym Encrypt) Public Key System

- Ensure public key is correct (not impostor)
- Certificate authorities
  - Certificate – package containing party's name and public key

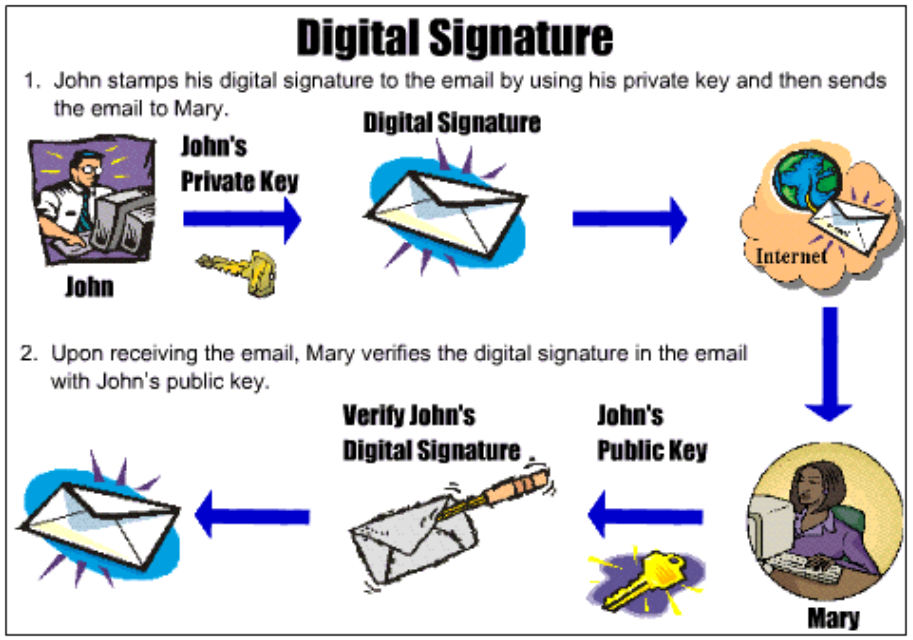




[What is a Certificate Authority? (globalsign.com)]

Digital Signature

- Previously, we encrypt using recipient's public key
  - Remember that recipient's private key is only known to recipient and is NOT circulated publicly
- To produce signature, sender encrypt using sender's private key



Since sender's private key is known only to sender and is NOT circulated publicly, recipient can be assured that the message sent by the sender originates from the sender!

Symmetric vs asymmetric cryptography

- Asymmetric cryptography may be more advanced than symmetric cryptography, but both are still in use today
- Two big trade-offs exist between symmetric and asymmetric cryptography:
  - **Speed**: Symmetric encryption has enormous advantage (both in encryption and decryption) because the keys used are much shorter and there is only one key.
  - **Security**: Symmetric cryptography carries a higher risk around key transmission as the same key is used and it must be shared with anyone who needs to decrypt.
- Symmetric cryptography applications
  - Banking: Encrypt credit card information
  - Data storage: Encrypt data stored on device or cloud
- Asymmetric cryptography applications
  - Digital signatures
  - Blockchain
  - Public key infrastructure (PKI)

Symmetric vs asymmetric cryptography

Symmetric	Asymmetric
Uses **same** key for encryption and decryption	Uses **different** keys for encryption and decryption
Key length is **shorter** than asymmetric encryption	Key length is **longer** than symmetric encryption
Faster than asymmetric encryption	**Slower** than symmetric encryption
Less secure than asymmetric	**More secure** than symmetric
Used for encrypting **large** amounts of data	Used for encrypting **small** amounts of data
Examples of applications: • Banking – encrypt credit card information • Data storage – encrypt data stored in decide or cloud	Examples of applications: • Digital signatures • Blockchain • Public key infrastructure (PKI)

Summary

- CIA
- Forms of Attack
  - Malwares, Botnets, DOS, etc.
- Protection
  - Authentication, Secured Connection, Encryption
- More in
  - ICT3103 Secured Software Development & Infocomm security
  - ICT2203 Applied Cryptography, ICT2205 Network Security

References

- *Chapter 8 Information Security*, An Invitation to Computer Science, 5th Edition, G. Michael Schneider, Judith L. Gersting, CENGAGE Learning
- *Public Key Cryptography: RSA Encryption Algorithm*, https://www.youtube.com/watch?v=wXB-V_Keiu8