SECURITY CONCEPTS

Two Significant Opportunities For Data to be Stolen
- interception of communication *(emails or electronic data is accessed by someone other than receiver)*
- infection of your computer

(not so) FUN FACT!
Computer is most vulnerable when communicating with other computers (i.e the internet)

ENCRYPTION

- *The 'scrambling' of text or data using a specified set of rules to ensure the privacy of data during communication, or for security purposes*

Local Encryption
- *use encryption software to protect the files on your local storage from being accessed by unauthorised people*
- Choice of whole hard drive or individual files
  - **Whole drive** – only need to enter the access key once when 'loading' encrypted drive
  - **Individual Files** - enter the key each time you access the file (slower but more secure)
- *Good form of protection for when computer is infected with malware that sends data off to a third party.*
-

Automatic Encryption
- Built into hardware and software
- Operates without user being aware
- Examples:
  - DRM (Digital Rights Management) - software to protect digital media (books, movies, etc) uses some form encryption to control access
  - ATM
  - Internet Browsers - *look for HTTPS protocol to see if encrypted*
  - Skype Calls
  - Online Storage Services - e.g Dropbox (not even employees can access files)
- *Used in situations that involve data communication*

SSL - SECURE SOCKETS LAYER

- *an encryption protocol which encrypts data sent over the internet. Used by websites for communicating sensitive information*
- **Why is it not plausible to use simple encryption?** The recipient and sender BOTH need the key to read the data.
- It, thus, uses public key encryption. It is used by many web browsers

PUBLIC KEY ENCRYPTION

- *a type of encryption where a generally available public key is used to encrypt data, but a different private key is needed to decrypt and read the data*

- ***PRIVATE KEY*** *- uses a single key. The key just be shared and kept private by both sender and receiver to encrypt and decrypt the message*

- Public key's differ in that one key is private and the other is public
- A mathematical algorithm is used to create two keys that are mathematically linked
  - The **public key** is used to encrypt the plain text
  - The linked **private key** is used to decrypt the text
- You cannot decrypt the message using the encryption key
- the encryption key can be made public - anyone can have it bc it can only be used to encrypt but not to decrypt
- *For instance, use John's public key to encrypt the message > send message to John > John uses his private key to decrypt*
- Examples *:*
  - **Websites** : https - SSL
  - **Whatsapp**

DIGITAL SIGNATURES

- *an electronic 'signature' used to identify and validate the sender of an electronic message or the 'signer; of an electronic document*
- Uses encryption techniques
- Provides proof that the message comes from the person who claims to have sent it
- *Signed with the sender's private key and verified with the sender's public key*
- Automatically time stamped to ensure authenticity
- **Make sure isn't altered?** Part of algorithm to form the signature is based on the contents of the data

DIGITAL CERTIFICATES

- *a Certificate issued by a trusted 3rd party to verify the identity of a person or an organisation, so that the person or organisation may be trusted for communication of sensitive information.*
- An essential part of the SSL encryption protocol
- Trusted 3rd Party - called a **Certificate Authority (CA)**
  - Thawte
  - Versign
- The certificate will be valid for a limited time

- **Contents** (**N**ot **E**very **O**nline **S**ervice **O**perates **D**iligently - which is why we need digital certificates)
    1. **N**ame of the Issuer (Certificate Authority)
    2. **E**xpiration Date of the Public Key
    3. **O**wner's Public Key
    4. **S**erial Number of The Certificate
    5. **O**wner's Name
    6. **D**igital Signature of the Issuer

- The certificate makes it possible for any browser to communicate with the server (of the website) and set up a public key encryption session (i.e SSL) in the background.
- If **ANY SINGLE** item of the data on the certificate does not match the communication session, the certificate is detected as invalid and the user us warned that they may be communicating with a site that is not what it claims to be

Pretty USELESS FACT!
Mark Shuttleworth is a South African entrepreneur who is a pioneer in the field of internet security and digital certificates