ENCRYPTION

What is it?

Welcome

- Who am I?
  - Jonathan A Burt BSc Cert Mgmt HND FIAP IEng MBCS CITP
    - Batchelor of Science Degree (Open)
    - Professional Certificate in Management
    - Higher National Diploma in Computing
    - Fellow of the Institute of Analysts and Programmers
    - Incorporated Engineer with the Engineering Council
    - Member of the British Computer Society
    - Charted IT Professional
    - PRINCE2 Practitioner
    - Foundation Certificate in IT Service Management (ITIL)
    - Certified Novell Administrator (v5.x)
  - 25+ years experience of working in IT, now retired.
  - Long time member of the Isle of Wight PC User Group!

Important!

- I cannot guarantee that all of the programs discussed are safe, and they are used at your own risk. I recommend that you investigate options based on your needs before using any software.
- Encryption is not fool-proof, and can failed. So always have backups of important data.
- Digital files which utilise Steganography can fail to reproduce the original message (if any) if they are edited, cropped, etc.
- Don’t do anything illegal! ☺

What is Encryption?

- With regard to cryptography, encryption is a process which converts the original representation of the information, known as **plaintext**, into an alternative form known as **ciphertext**.

- It is a way to protect your data, whether…
  - saved on your computer
  - saved on an external drive
  - emailed to someone
  - purchasing online (i.e. https)
  - remote access to networks (i.e. VPNs).

The History of Encryption

- One of the earliest forms of encryption is symbol replacement, which was first found in the tomb of **Khnumhotep II**, who lived in 1900 B.C. Egypt.
  - Symbol replacement encryption is “non-standard,” which means that the symbols require a cipher or key to understand. This type of early encryption was used throughout Ancient Greece and Rome for military purposes.
  - One of the most famous military encryption developments was the **Caesar Cipher**, which was a system in which a letter in normal text is shifted down a fixed number of positions down the alphabet to get the encoded letter. A message encoded with this type of encryption could be decoded with the fixed number on the Caesar Cipher.

The History of Encryption

- Around 800 A.D., Arab mathematician **Al-Kindi** developed the technique of frequency analysis - which was an attempt to systematically crack **Caesar ciphers**.
- This technique looked at the frequency of letters in the encrypted message to determine the appropriate shift.
- This technique was rendered ineffective after the creation of the **Polyalphabetic cipher** by **Leone Alberti** in 1465, which incorporated different sets of languages.
- In order for frequency analysis to be useful, the person trying to decrypt the message would need to know which language the sender chose.

The History of Encryption

- Around 1790, **Thomas Jefferson** theorized a cipher to encode and decode messages in order to provide a more secure way of military correspondence. The cipher, known today as the **Wheel Cipher** or the **Jefferson Disk**, although never actually built, was theorized as a spool that could jumble an English message up to 36 characters. The message could be decrypted by plugging in the jumbled message to a receiver with an identical cipher.

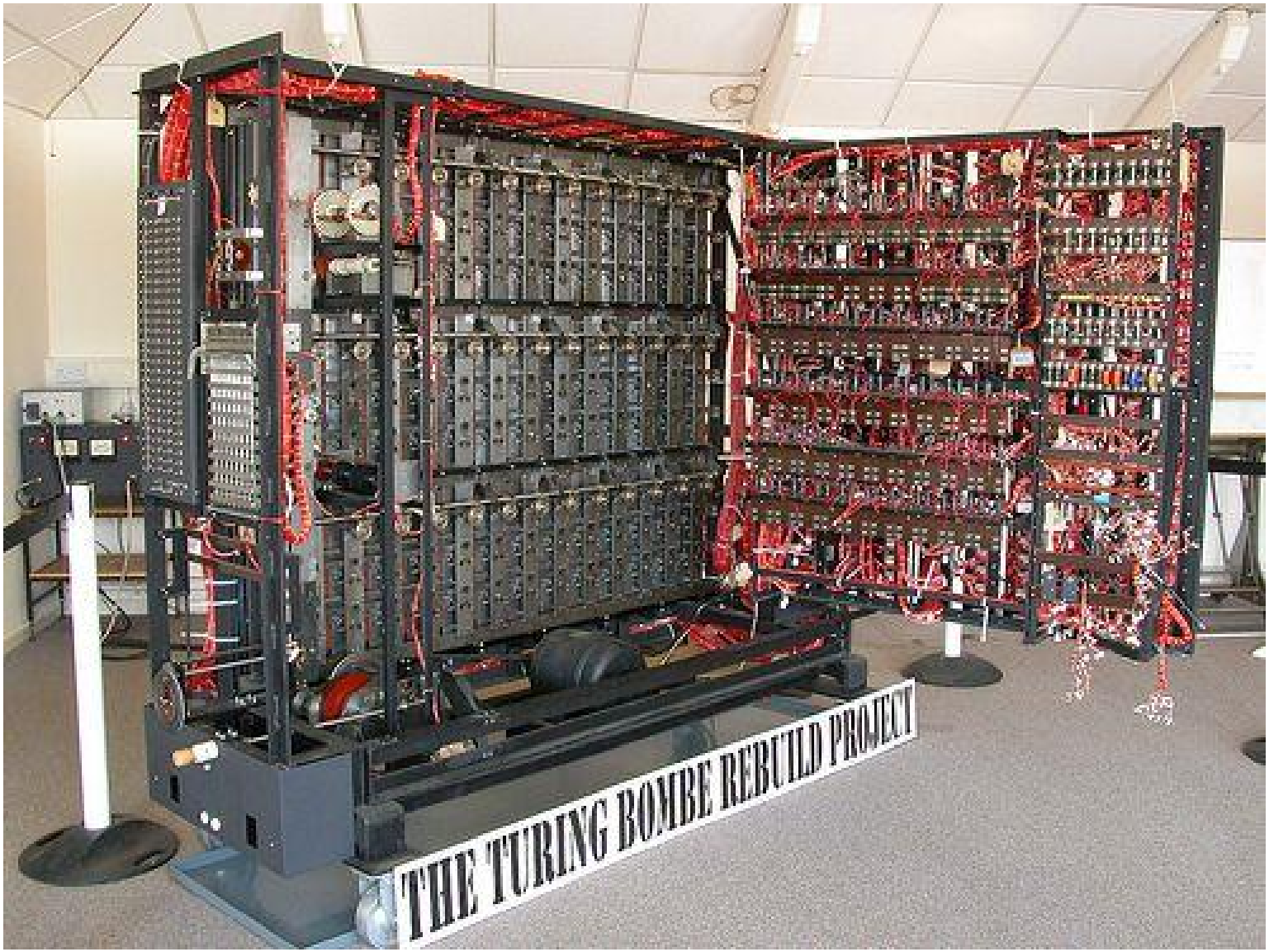
- A similar device to the **Jefferson Disk**, the **M-94**, was developed in 1917 independently by US Army Major **Joseph Mauborne**. This device was used in U.S. military communications until 1942.

- In World War II, the Axis powers used a more advanced version of the **M-94** called the **Enigma Machine**. The **Enigma Machine** was more complex because unlike the **Jefferson Wheel** and the **M-94**, each day the jumble of letters switched to a completely new combination. Each day's combination was only known by the Axis, so many thought the only way to break the code would be to try over 15,000,000,000 combinations within 24 hours. The Allies used computing power to severely limit the amount of reasonable combinations they needed to check every day, leading to the breaking of the **Enigma Machine**.

Bletchley Park

- The IW PC User Group visited Bletchley Park on the 9th July 1999, not long after it opened!

The Bombe

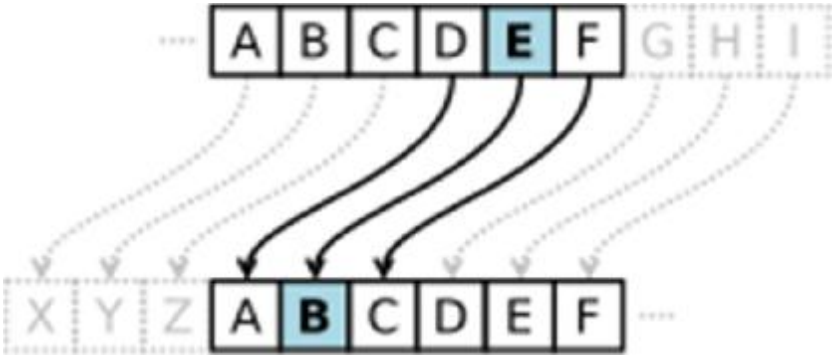


The History of Encryption

- Today, encryption is used in the transfer of communication over the Internet for security and commerce.
- As computing power continues to increase, computer encryption is constantly evolving to prevent attacks.
- Computing allows for much more complex encryption methods, than the “old fashion” manual processes.

Caesar Cipher

- One of the simplest and most widely known encryption techniques.
  - The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions.
  - For instance, here is a **Caesar cipher** using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):



Caesar Cipher

- Plain Alphabet:
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cipher Alphabet:
  - XYZABCDEFGHIJKLMNOPQRSTUVW

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

Book Cipher

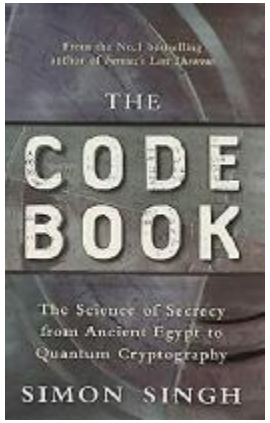
- A **book cipher**, or **Ottendorf cipher**, is a cipher in which the key is some aspect of a book or other piece of text.
  - Books, being common and widely available in modern times, are more convenient for this use than objects made specifically for cryptographic purposes.
  - It is essential that both correspondents not only have the same book, but the same edition.
- The Bible and a Dictionary are widely available books which have been used for this purpose.
  - In the American Revolution, **Benedict Arnold** used a book cipher, sometimes known as the **Arnold Cipher**, which used **Sir William Blackstone's Commentaries on the Laws of England** as a key text.

Book Cipher

- So using **The Code Book**, as my **Book cipher**, I send someone the following code.

49 6 66 74 11 7 27 14

- The Code Book: The world is crazy
- Rainbow Six: Tell at John could
- The Shepherd's Crown: It was his at



Code Words

- Another form of encryption, which requires both parties to have a code book.
  - This way innocent words would have alternate meanings.
  - They could be hidden in a letter (say, agreed before hand that every 6 word is a code word), or just send as a simple code word.
  - You could even encrypt the code words further, which makes decrypting harder, as decryption cracking often looks for repeating patterns, which would not appear in a selection of random code words.

“Key” Encryption

- Symmetric key
  - In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication. The German Enigma Machine utilized a new symmetric-key each day for encoding and decoding messages.
- Public Key
  - In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.
  - Public-key encryption was first described in a GCHQ secret document in 1973.
  - Pretty Good Privacy (PGP) was written in 1991 by Phil Zimmermann, and distributed free of charge with source code. This brought Public Key encryption to the masses for free!

Limitations

- As computing power increased over the years, encryption technology has only become more advanced and secure. However, this advancement in technology has also exposed a potential limitation of today's encryption methods.
- The length of the encryption key is an indicator of the strength of the encryption method.
  - For example, the original encryption key, DES (Data Encryption Standard), was 56 bits, meaning it had 2^56 combination possibilities.
  - With today's computing power, a 56-bit key is no longer secure, being vulnerable to hacking by brute force attack.
  - 2^56 is 72,057,594,037,927,936 unique combinations!

Limitations

- The length of the encryption key is an indicator of the strength of the encryption method.
  - Today the standard of modern encryption keys is up to 2048 bit with the RSA (Rivest–Shamir–Adleman) system.
  - Decrypting a 2048 bit encryption key is nearly impossible in light of the number of possible combinations. However, quantum computing is threatening to change this secure nature.
  - 2^2048 has an amount of unique combinations equal to a number which is 617 digits long!

Limitations

- The actual degree of security achieved over time varies, as more computational power and more powerful mathematical analytic methods become available.
- For this reason, cryptologists tend to look at indicators that an algorithm or key length shows signs of potential vulnerability, to move to longer key sizes or more difficult algorithms.
- For example, as of May 2007, a 1039-bit integer was factored with the special number field sieve using 400 desktop computers over 11 months.
  - The factored number was of a special form; the special number field sieve cannot be used on RSA keys.
  - The computation is roughly equivalent to breaking a 700 bit RSA key.
  - However, this might be an advance warning that 1024 bit RSA used in secure online commerce should be deprecated, since they may become breakable in the near future.

Wi-Fi Encryption - WEP

- Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.
  - Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network.
  - WEP, recognizable by its key of 10 or 26 hexadecimal digits (40 or 104 bits), was at one time widely in use and was often the first security choice presented to users by router configuration tools.
- In 2005, a group from the U.S. Federal Bureau of Investigation gave a demonstration where they cracked a WEP-protected network in **three minutes** using publicly available tools!

Wi-Fi Encryption – WPA v1

- The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard.
  - WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999.
  - However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.
- The WPA protocol implements much of the IEEE 802.11i standard.
  - Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA.
  - WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

Wi-Fi Encryption – WPA v2

- Ratified in 2004, WPA2 replaced WPA.
  - WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i.
  - In particular, it includes mandatory support for CCMP, an AES-based encryption mode.
  - Certification began in September, 2004.
  - From March 13, 2006 to June 30, 2020, WPA2 certification was mandatory for all new devices to bear the Wi-Fi trademark.

Wi-Fi Encryption – WPA v3

- In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. Certification began in June, 2018.
  - The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.
  - The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode and forward secrecy.
  - The Wi-Fi Alliance also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.
  - Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.

Quantum

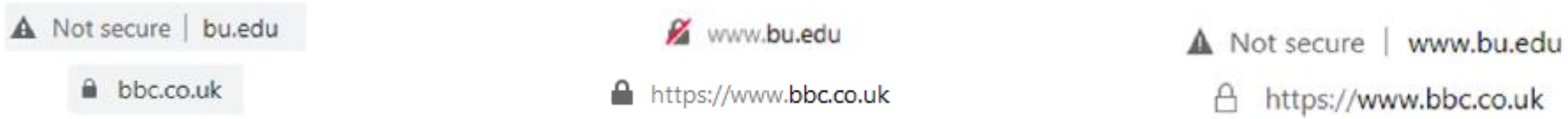
- Quantum computing utilizes properties of quantum mechanics in order to process large amounts of data simultaneously.
  - Quantum computing has been found to achieve computing speeds thousands of times faster than today's super computers.
  - This computing power presents a challenge to today's encryption technology.
  - For example, RSA encryption utilizes the multiplication of very large prime numbers to create a semiprime number for its public key. Decoding this key without its private key requires this semiprime number to be factored, which can take a very long time to do with modern computers. It would take a super computer anywhere between weeks to months to factor this key.
- However, quantum computing can use quantum algorithms to factor this semiprime number in the same amount of time it takes for normal computers to generate it.
  - This would make all data protected by current public-key encryption vulnerable to quantum computing attacks. Other encryption techniques like elliptic curve cryptography and symmetric key encryption are also vulnerable to quantum computing.

Quantum

- While quantum computing could be a threat to encryption security in the future, quantum computing as it currently stands is still very limited.
- Quantum computing currently is not commercially available, cannot handle large amounts of code, and only exists as computational devices, not computers (as we know them).
- Furthermore, quantum computing advancements will be able to be utilised in favour of encryption as well.
  - The National Security Agency (NSA) is currently preparing post-quantum encryption standards for the future.
  - Quantum encryption promises a level of security that will be able to counter the threat of quantum computing.

Encryption and Browsing

- By default, whenever you browse the Internet from one of the many browsers available you are usually browsing in an insecure manner. However this is slowly changing.
  - This means, that any data you enter, for example name, address, email, credit card number, would be sent as plaintext between your PC and the server hosting the webpage.
- However, if you are using **https://** then your data is being encrypted on your device, and then decrypted on the server, thus protecting your privacy.
  - A visual way to prove you are secure is to look for the padlock next to the website address in your browser.



Encryption and Browsing

- So how does it work?
  - Browser connects to server Using SSL (https)
  - Server Responds with Server Certificate containing the **public key** of the web server.
  - Browser verifies the certificate by checking the signature of the **Certificate Authority**.
  - Browser uses this **Public Key** to agree a **session key** with the server.
  - Web Browser and server encrypt data over the connection using the **session key**.

Steganography

- The practice of concealing messages or information within other non-secret text or data.
  - For example, a photo or image on a webpage could contain a hidden message.
  - When you think how many websites and forums have pictures, there are billions of places where messages could be hidden!
  - In 2014, according to Mary Meeker's annual Internet Trends report, people uploaded an average of 1.8 billion digital images every single day.
- In June 2010, the FBI caught a Russian spy ring which was using **steganography** to send messages to each other on public websites and forums!

Full Disk Encryption

- Full disk encryption (FDE) is a storage encryption technology that secures a desktop or laptop computer by encrypting all the data at rest on its hard drive.
  - This includes end-user files and application settings, as well as application and operating system (OS) executables.
- The principal concern with data at rest is that a device containing sensitive information could be lost or stolen, allowing a person with malicious intent to recover that data.
  - Any organisation of any size with sensitive data at rest to protect (e.g., financial information, customer records, medical records and other sensitive data that could lead to major breaches and cost thousands or millions of dollars) can benefit from using full disk encryption software.

FDE Software

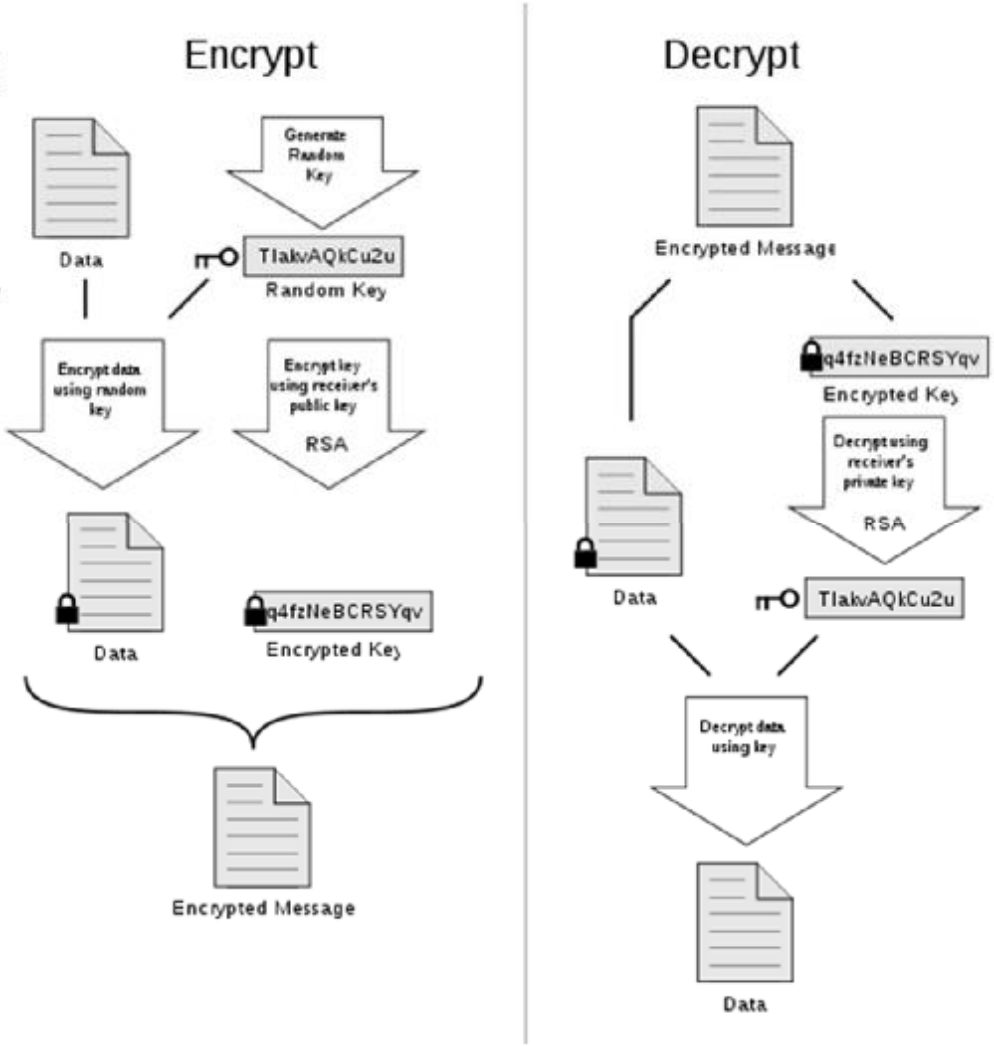
- There are many paid software solutions out there which offer Full Disk Encryption, for example:
  - Windows 10 Pro (BitLocker)
  - Dell Data Protection Encryption
  - Check Point Full Disk Encryption
  - McAfee Complete Data Protection
  - Sophos SafeGuard
  - Symantec Endpoint Encryption
  - and many more.

FDE Software

- There are many free software solutions out there which offer Full Disk Encryption, for example:
  - DiskCryptor (opensource)
  - TrueCrypt (opensource) NO LONGER SECURE
  - VeraCrypt (opensource)

File and Email Encryption

- Sometimes you might just want to encrypt a single file or email, and don't need Full Disk Encryption. Like with FDE, there are numerous programs available to assist with this.
- The most commonly known is PGP (Pretty Good Privacy) which was developed in 1991, as a **public key** encryption system.



Questions?

Does anyone have any questions?

Further Information

- Wikipedia
  - https://en.wikipedia.org/
- Lots of useful tutorials
  - http://www.howtogeek.com/
- TechRadar has a good selection of reviews.
  - http://www.techradar.com/
- LinkedIn
  - https://www.linkedin.com/in/jaburt/