

**NOVEMBER 2018**

**PRODUCTION**

**LOGBOOK**

**LEVEL 3 EXTENDED PROJECT (2935-03)**

**CANDIDATE RECORD FORM, PRODUCTION LOG AND ASSESSSMENT RECORD**

|  |  |
| --- | --- |
| **Candidate’s Full Name:** | **Jack** |
| **City & Guilds Registration Number:** | **GWP0270** |
| **Centre Name:** | **Qufaro** |
| **Centre Number:** | **006820** |

**Notice to candidate:** The work you submit for assessment must be your own. If you copy from someone else or allow another candidate to copy from you, or if you cheat in any other way, you may be disqualified.

**To be completed by the candidate**

1. Have you received any help or information from anyone other than you subject teacher/tutor(s) in the production of this work?

Yes No

1. If you have answered yes, give details below and on a separate sheet if necessary.

|  |
| --- |
| N/A |
|  |
|  |
|  |

1. Any books, leaflets or other materials (e.g. DVDs, software packages, Internet information) used to help you complete this work and not clearly acknowledged in the work itself must be listed below. Presenting materials copied from books or other sources **without acknowledgement** will be regarded as deliberate deception.

|  |
| --- |
| All sources are acknowledged in the references and bibliography sections of the essay. |
|  |
|  |
|  |

**Candidate’s Declaration:** I have read and understood the above and can confirm that I have produced the attached work without assistance other than that which is acceptable under the scheme of assessment.

Candidate’s Signature: **Jack**  Date: 7/11/23

**Centre Assessor’s Declaration:** I confirm that the candidate’s work was conducted under the conditions laid out by the specification. I have authenticated the candidate’s work and am satisfied that to the best of my knowledge the work produced is solely that of the candidate. Assessment was conducted under the specified conditions and context, and is

valid, authentic, reliable, current and sufficient.

Centre Assessor’s Signature: Date:

**SUBMISSION CHECKLIST**

Candidate’s Full Name: City & Guilds Registration Number:

**Please note:** All elements of the Project are compulsory. Failure to complete or submit an element may result in a mark of zero being awarded.

|  |  |  |
| --- | --- | --- |
| **To include** | **Completed** | **Additional notes** |
| A signed and completed *Candidate record form, production log* and *assessment record* |  | This document. All pages must be completed by the candidate, except for pages 3, 7, 8 and 14 |
| Evidence of the project outcome |  | E.g. photographs of artefact or production; a piece of creative writing (artefact); research based written report; CD/video/DVD of performances or activities; audiotape/multimedia presentation |
| Research based written report |  | If the project outcome is an artefact or a production, **an accompanying research based written report is required** |
| Evidence of a presentation within the production log |  | Presentation on the project process. Where the project outcome is a presentation, a presentation on the project process still has to be completed |

**RECORD OF MARKS**

Candidate’s Full Name: City & Guilds Registration Number:

**To be completed by the supervisor**

Marks must be awarded in accordance with the instructions and criteria in Section 4 of the Qualification Handbook.

Summary information to show how the marks have been awarded should be given in the spaces below in addition to comments in other pages of this document and any supporting information in the form of annotations on the candidate’s work.

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment outcome** | **Max Mark** | **Mark awarded** | **Additional comments** |
| AO1 Manage | 10 |  |  |
| AO2 Use resources | 10 |  |  |
| AO3 Develop and realise | 20 |  |  |
| AO4 Review | 10 |  |  |
| **Total** | **50** |  |  |

**Concluding comments:**

|  |
| --- |
|  |
|  |
|  |
|  |

**Outline details of taught skills:** Record here details of relevant skills taught in a class/group and details of relevant skills taught individually to this candidate as described in the specification. Continue on a separate sheet if necessary.

|  |
| --- |
|  |
|  |
|  |
|  |

**Supervisor’s declaration:** I confirm that no work assessed for the award of the marks above is also to be submitted, or has been submitted, for any other accredited qualification(s).

**Supervisor’s Signature:**   **Date:**

**CONTENTS**

**Candidate’s Full Name:**  **City & Guilds Registration Number:**

**To be completed by the candidate**

**Extended Project working title**

|  |
| --- |
| How has encryption evolved and what does the future hold for it in the age of quantum computing? |
|  |

**Planned form of evidence submitted for project**

|  |
| --- |
| **Essay** |
|  |

This document consists of the pages listed below. Additional journal material, planning evidence, research evidence, presentation evidence, records of meetings with your supervisor and review material may be added.

|  |  |  |
| --- | --- | --- |
| **Page No** | **Title** | **Date Completed** |
| 2 | Candidate declaration | /23 |
| 3-4 | Submission checklist and Record of marks |  |
| 5 | Contents | 6/11/23 |
| 6 | Record of initial planning | 15/2/23 |
| 7-9 | Project proposal and approval (Part A, B, and C) | 10/3/23 |
| 10 | Planning review (start of project) | 25/6/23 |
| 11 | Mid-project review | 12/9/23 |
| 12 | End-of-project review | 5/10/23 |
| 13 | Summary | 2/11/23 |
| 14-15 | Presentation record (Part A and B) | 20/10/23 |
| 16 | Reflection | 5/11/23 |

Is this extended project part of a group project?

**Yes No**

**Extended Project final title**

|  |
| --- |
| “How has encryption evolved and can it survive in the age of quantum computing?” |
|  |
|  |
|  |

**RECORD OF INITIAL PLANNING**

**RECORD OF INITIAL PLANNING**

**Candidate Full Name:** Jack **City & Guilds Registration Number:** GWP0270

**To be completed by the candidate**

**Note:** This section records initial meeting(s) with your supervisor to agree your project proposal.

|  |  |
| --- | --- |
| **Your first idea for topic (to include overall aim)** | * How has encryption evolved and what does the future hold for it in the age of quantum computing? * How has encryption evolved and will secure encryption be achievable in the age of quantum computing? * How has encryption evolved and is truly secure encryption possible in the age of quantum computing?   My aim is to determine whether secure encryption will be achievable in the age of quantum computing. |
| **Your first ideas for research and development of your project** | * History of encryption and its uses – the cracking codebook (Simon Singh), articles and web pages on the internet. * An overview of quantum computing, how it is different and why it is superior to conventional computation in certain areas – Computing with Quantum Cats (John Gribbin), articles and web pages on the internet. * Why may quantum computers pose a threat to modern encryption techniques. * What methods could be used to make encryption secure against quantum computers? * Is truly secure encryption possible in the age of quantum computing? * Cryptography Apocalypse - Preparing for the day When Quantum Computing Breaks Today’s Crypto (Roger A. Grimes) |
| **Your supervisor’s main comments and advice** | * This looks like a great topic, providing ample opportunity to research interesting technologies and draw sound conclusion * Title 3 looks good * You’ve provided a good range of research options * Could you arrange an interview with an expert in quantum computers to provide additional facts for your report |
| **Changes, clarifications or additions you have made as a result of your discussion with your supervisor** | * As a result of my discussion, I have decided to focus on topic 3 * I will consider trying to obtain an interview with an expert in the field of quantum computing |

**Supervisor’s Signature:**  **Date:**

**PROJECT PROPOSAL – PART A**

**Candidate’s Full Name:** **Jack**  **City & Guilds Registration Number:** **GWP0270**

**To be completed by the candidate**

|  |  |
| --- | --- |
| **Title of Extended Project** Present the topic to be researched in the form of a short statement/question/hypothesis with clear focus | **How has encryption evolved and is truly secure encryption possible in the age of quantum computing?** |
| **Provide a brief outline of the research or activity/ task to be carried out and sources to be consulted with** | **I will research the history of encryption. I need to read relevant books to gain an understanding of quantum computers and how they are superior to modern computers. Finally, I will research the threat quantum computers pose to modern encryption standards and how this can be mitigated.**  **Sources - The Cracking Codebook (Simon Singh), A shortcut through time - the path to the quantum computer (George Johnson), The God Effect (Brian Clegg), The Quantum Universe: everything that can happen does happen (Brian Cox, Jeff Forshaw), Computing with Quantum Cats (John Gribbin), Cryptography apocalypse (Roger A Grimes), RSA Security’s Official Guide to Cryptography (Steve Burnett, Stephen Paine).**  **I will also find journal articles and web pages on the internet to supplement my research.** |
| **Provide a brief outline of the course of study or area(s) to which the topic relates** | **I have completed the Cyber EPQ course which contained a small section on encryption. I am looking to extend my knowledge and understanding of this subject, and look at the issues quantum computing could create.** |
| **Provide a brief outline of any specific resources and/or equipment you may require, as appropriate** | **The resources I require are: books, journal articles, web pages and access to a computer.** |
| **Provide a brief outline of your proposed action** | **I will begin by reading all the books recorded in my sources list. Following on from this, I will then look for relevant journal articles and web pages online to extend my research. Once I have completed most of the research, I will begin to plan the structure of my written report.** |

**Candidate declaration:** I confirm that I have read and understood City & Guilds regulations relating to unfair practice as set out in the notice to candidates below.

**Notes to candidates:** You must not submit work which is not your own; lend work to other learners; allow other learners access to, or the use of, your own independently sourced material (this does not mean that you may not lend your books to another learner, but you should be prevented from plagiarising other learners’ research); include work copied directly from books, the internet or other sources without acknowledgement or an attribution; or submit work typed or word processed by a third person without acknowledgement. Failure to comply with these considerations may result in unfair practice and subsequently being disqualified.

**Candidate’s Signature: Jack**  **Date: 25/02/2023**

**PROJECT PROPOSAL – PART B**

**Candidate’s Full Name: Jack**  …………………………..**City & Guilds Registration Number: GWP0270**

**To be completed by the supervisor**

Please comment below on the validity and feasibility of the proposal (project proposal Part A).

**Supervisor’s comments**

|  |  |
| --- | --- |
| Comment on the clarity and focus of the title chosen | The candidate has provided a good title, with a clear focus on encryption, looking at the evolution over time and the threats of quantum computing. |
| Indicate the relation to, and development/extension outside of, the main course(s) of study or interest | This is clearly linked to the CyberEPQ modules, with some link to the encryption unit in Computer Science. |
| Comment on the suitability of the proposed initial sources and research base | A good plan has been presented on what needs to be researched, along with a good list of sources to begin the research. |
| Confirm that project is feasible in the proposed timescale and/or indicate any potential difficulties, to include specified resources/equipment | The project is feasible in the given timeframes. |
| Outline the scope to produce a project that meets the assessment objectives (**Section 4** of the Qualification Handbook) | This proposal provides more than enough scope to: design, plan and complete an  individual project (A01); identify, obtain and analyse resources (A02); use a range  of skills when completing the project (A03); and review the project and process  (A04) |
| Indicate proposed form and date of the presentation | The presentation will take the form of a PowerPoint presentation followed by a  Q&A, scheduled for the summer term, sometime in July. The exact date is yet to be determined. |

**Indicate the expected format of the project product that will be submitted for assessment**

|  |  |
| --- | --- |
| Written Report | X |
| Live performance (e.g. music, drama, theatre, substantial presentation) plus written report |  |
| Electronic format (e.g. CD, DVD, video, programme) plus written report |  |
| Artefact (e.g. prototype, model, artwork) plus written report |  |
| Other |  |

X

**Is this Extended Project part of a group project? Yes No**

**If Yes, identify group members below and confirm that there is a defined Yes No**

**Individual contribution by the candidate.**

**Candidate’s Name: Jack**   **Registration Number: GWP0270**

**Supervisor’s Signature R. Jarvis**  **Date: 27/02/2023**

**PROJECT PROPOSAL – PART C**

**Candidate’s Full Name:** **: Jack**  **City & Guilds Registration Number: GWP0270**

**Supervisor’s Full Name:**

**To be completed by the Centre Coordinator**

Comment on the feasibility and acceptability of the proposal (Project Proposal parts A and B) as an Extended Project.

**Centre Coordinator’s comments:**

|  |
| --- |
| * **The student’s working title of the project successfully allows higher – level concepts and skills in the assessment objectives such as analysing, evaluating and explaining and is not limited to simply describing and narrating their chosen topic area.** * **The student has organised their planning to ensure that the project can be feasibly finished within the timeline for submission.** * **The working title and proposed action are clear and focuses on the issue and will be feasible regarding the resources available as well as being able to keep within the boundaries of the required word limit.** * **The student has provided a clear and varied list of resources and should not experience any difficulties in accessing the sources to research their project.** * **The student will be capable of investigating and researching the topic independently.** * **The project appears to allow the topic to be approached in an impartial and balanced way.**      * **The student is unlikely to face difficulties understanding the concepts associated with the project topic.** * **There are no apparent risk elements concerning this project.**   **ADDITIONAL COMMENTS** |
|  |

|  |
| --- |
| **Approved**  **√** |
| **Approved subject to the implementation of the centre coordinator’s recommendations** |
| **Resubmission required** |

**Coordinator’s Full Name:** Nicky Bodily

**Coordinator’s Signature:** Nicky Bodily **Date**: March 10th 2023

**PLANNING REVIEW:**

**AT THE START OF YOUR PROJECT**

**Candidate’s Full Name:** Jack …………… **City & Guilds Registration Number: :** **GWP0270**

**To be completed by the candidate**

This page records your outline plan at the start of your work.

|  |  |
| --- | --- |
| **Outline the steps in your project. You might want to include:**   * What do you want to achieve? * What are your timescales? * What resources will you use? * Who can support you to achieve your objectives? | How has encryption evolved and what does the future hold for it in the age of quantum computing?  Introduction   * What is encryption? * Government definitions of encryption based on standards - <https://csrc.nist.gov/glossary/term/encryption#:~:text=2%20under%20Encryption-,The%20process%20of%20changing%20plaintext%20into%20ciphertext%20using%20a%20cryptographic,purpose%20of%20security%20or%20privacy> * What is encryption used for, future possible uses   + Government definition of cryptography with various standards - <https://csrc.nist.gov/glossary/term/cryptography#:~:text=Definition(s)%3A,or%20prevent%20their%20undetected%20modification>. * What is cryptography? * Cryptography vs encryption * Define the terms (possibly put some or all of this into glossary?) – ciphers vs codes   + <https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes>   + <https://www.encyclopedia.com/social-sciences-and-law/law/crime-and-law-enforcement/codes-and-ciphers> * Steganography vs cryptography * Two branches of cryptography – transposition vs substitution   + <https://www.tutorialspoint.com/difference-between-substitution-cipher-technique-and-transposition-cipher-technique>   + <http://ijrar.com/upload_issue/ijrar_issue_20543567.pdf> * The security of ciphers – unconditional vs conditional security   + <https://en.wikipedia.org/wiki/Information-theoretic_security> * Semantic security   + <https://en.wikipedia.org/wiki/Semantic_security> * Entropic security   + <https://en.wikipedia.org/wiki/Entropic_security> * Monoalphabetic vs polyalphabetic vs polygraphic   + Monoalphabetic e.g. Affine, atbash, Caesar   + Homophonic e.g. the Beale ciphers   + Polyalphabetic e.g Vigenère, autokey, running key cipher, Porta, Beaufort, Gronsfeld   + Polygraphic e.g. 4 square cipher (like playfair), playfair, hill cipher * Block vs stream ciphers   Part 1 History of ciphers  Earliest ciphers and their uses   * 4000 years ago, the earliest written evidence of encryption was in ancient Egypt – tomb of nobleman Khnumhotep II held a script telling of his deeds in life – unusual hieroglyphs however obscured the original meaning of the text. Encryption in ancient Egypt was mainly used to protect knowledge as education was a privilege only available to the highest circles of society. It was also used for religious reasons such as to discuss taboos. * Scytale – transposition – ancient spartan – 7th century BC – early version of railfence cipher – the scytale is actually the rod of specific diameter used to perform a transposition cipher. * Rail fence cipher – route cipher (with scytale as all transpositions and forms of each other) * 3rd century BC – Polybius square – Cleoxenus and Democleitus were historians and Cleo wrote a lost History Of The Persians. Polybius mentions them as inventors of a telegraphic communications system that relied on smoke/fire signals for transmitting letters from the Greek alphabet. Polybius says that he perfected it and made it capable of dispatching with accuracy every kind of urgent message, but in practice it requires care and exact attention. The improvement he made in around 134 BC led to the Polybius Square, using torches to transmit letters. * Atbash cipher - found in ancient Israel, originally developed for use with the Hebrew alphabet. In the Book of Jeremiah, possibly composed about 300 BC by a Jew in Babylon. Jeremiah was a prophet, book has a picture of how disobedience leads to destruction. The Book of J is the 2nd of the latter prophets in the Hebrew Bible and the second of the prophets in the Christian old testament – find example of encryption? * Roman encryption – Caesar cipher – (sometimes with key word) - Used by Julius Caesar circa 60 BC – ROT13 * (Roman times) Latin squares – a series of 5 letter words arranged in a square, a transposition cipher as when letters are rearranged, they form Christian messages – they were put on the sides of Roman villas that offered refuge to Christians, who were the only people who knew how to transpose the letters. Example in Manchester Museum. * 4th Century AD – Kama-sutra cipher – one of the earliest substitution ciphers – described in Kama-sutra, written by Brahmin scholar Vatsyayana, based on manuscripts dating back to the 4th century BC. It recommends women study 64 arts including cooking, dressing, chess etc. 45 on the list is mlecchita-vikalpa, the art of secret writing, to help women hide of details of their liaisons. * Early 15th century -> late 18th century – nomenclator ciphers were used for diplomatic correspondence and espionage. They were being routinely broken by the mid-16th century. The Rosignoles’ Great Cipher used by Louis XIV of France was an example. After it went out of use, messages in French archives were unbreakable for several hundred years * 1467 – the Alberti cipher – one of the earliest polyalphabetic ciphers – invented by Leon Battista Alberti – for the next 100 years, the significance of using multiple substitution alphabets was missed by almost everyone? * 1550 Cardano invented the Cardan grille, Renaissance – technically a form of stenography where the message is concealed, but the grille itself could be considered to be a key * 1553 Giovan Battista Bellaso – Vigenère cipher (misattribute to Vigenère as he invented/improved upon it with the similar autokey cipher) - first cipher to use proper encryption key. At the time and for about 3 centuries it was believed to be unbreakable – eventually called the “unbreakable cipher”, and wasn’t broken until 1863 by Kasiski. Beaufort, Gronsfeld, and Porta ciphers are all variations. * The running key cipher – similarly to Vigenère, but rather than using a short repeating key it uses a long key e.g. an excerpt from a book. If the key is statistically random, it is a form of one-time pad. * 1586 Autokey cipher, by Vigenère – more secure than other polyalphabetic ciphers as the key comes from the plaintext and thus does not repeat. * 1586 Mary Queen of Scots – simple substitution cipher used to send treasonous letters. It was broken by Thomas Phelippes (Working for Walsingham) using frequency analysis and she was killed. Used symbols as substitutes instead of letters, and used special symbols for common words. There were also 4 nulls – symbols that had no meaning and were just there to confuse people trying to decipher it. Actually, they broke a message sent to her by a plotter, Babington, asking for her endorsement of a plot, and waited for her reply, as supporting the plot would allow them to execute her. * 1605 Francis Bacon – Baconian cipher – method of steganographic message encoding – it is categorised as both a substitution cipher (in plain code) and a concealment or null cipher – a null cipher is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material – today it is regarded as simple form of steganography, which can be used to hide ciphertext. (using the 2 typefaces) - the message is hidden in the presentation of the text rather than in its content, and is also in binary, forming the encryption/substitution part of the cipher. * 18th century Pigpen cipher – used by Freemasons to keep their records private – substitution cipher – letters substituted for symbols. Letters are put in grids and crosses, they are replaced by a drawing of the part of the grid around the message * 1854 Charles Wheatstone – Playfair cipher – (called that because Playfair promoted its use) – polygraphic substitution – encrypts pairs of letters * 4 square cipher is like Playfair but has 4 squares not one * 1819-21 Beale ciphers – an example of a book cipher (homophonic) – story of buried treasure – in 3 parts – one keyed to the declaration of independence and solved, the others unsolved.   Monoalphabetic and some simpler polyalphabetic substitution ciphers obsolete from this point.  WW1 and WW2 cryptography   * Playfair cipher used in 2nd Boer war and ww1 * Rotor machine invented in several places at once 1915-17 * 1917 – American Edward Hebern invented electro-mechanical machine (rotor machine) in which the key is embedded in a rotating disc – called Hebern rotor machine. First time electrical circuitry was used in a cipher device. In WW1 everyone could read everyone else’s simple ciphers – this lead to the development of rotor machines. Combined typewriters with rotating cipher discs, that would rotate periodically to change which letters of the alphabet corresponded. He tried to sell it to the US military – they refused, as they broke the cipher but did not tell him so they could use the experience to help them break similar ciphers like enigma. * 1917 – Gilbert Sandford Vernam invernted the Vernam cipher/stream cipher. The Vernam cipher and one time pad are very similar in effect – major difference is the one time pad implements an XOR for the first time and dictates that a truly random stream cipher be used for the encryption. * 1918 – Enigma machine invented by Arther Scherbius, which used several rotors and was used by the Germans in WW2. It was initially broken by the Polish at the beginning of WW2, using electromechanical devices called Bombes. When Poland was overrun by the Nazis, they sent the Bombes to Britain (Bletchley park) so they could continue to be used against Germany. However, part way through WW2, Germany upgraded the enigma machine with 2 more rotor possibilities, so the bombes had to be redesigned. * Columnar transposition WW1 * Double transposition cipher – one of the most secure hand-ciphers, used in WW2 – just columnar transposition applied twice. * July 9th, 1941 – Enigma broken * Hitler used Lorenz cipher – more complex rotor machine – early stream cipher * The people at Bletchley park broke this by building Colossus, the world’s first computer, which was designed to search through all the possible keys to the Lorenz cipher to find the correct combination. * 1944 Rasterschlussel 44 was a transposition based grille cipher used by the German Wehrmacht in WW2 * British used one-time pad, theoretically unbreakable – look into if still used now in digital form. * Claude E Shannon – “A Mathematical Theory of Cryptography” – proved that the one time pad was unbreakable, and that any unbreakable system must have same principles – “the key must be truly random, as large as the plaintext, never reused in whole or part, and kept secret” (Wiki). * Simplest one time pad is convert letters into numbers, 1-26. Write another series of numbers above each number. For each letter, add the 2 numbers. This is the ciphertext. As the person trying to break it knows neither the original number corresponding to the letter, nor the number you added, it cannot be broken. Generally there are 3 or 4 pieces of information, one is the plaintext, one is the ciphertext, and one is the key (or there are 2 pieces of information that together make the key as in RSA). However, as your opponent only has the ciphertext, but at least 2 pieces of information are required to decrypt the text, it cannot be decrypted. * Why are one time pads not used everywhere despite being unconditionally secure – difficulties of distributing keys and the need for public key infrastructure. However, PKI is slow, and so to take advantage of both use PKI to transmit the key to a private encryption, which is then much faster and unconditionally secure. However, the public key cipher can only be conditionally secure, as in theory the private key could be obtained from the public key if you had enough computing power.   Modern cryptography (computer based)   * 1953 – possible first use of the concept of the hash function at IBM * IBM forms crypt-group in the 1970s with other leading companies, due to the requirement for an effective and standardised encryption algorithm– developed lucifer encryption, using block cipher – became DES. * Modern bit oriented block ciphers like DES and AES can be seen as substitution ciphers on a massive binary alphabet. * Early 1970s – invention of public key infrastructure at GCHQ, but kept secret for national security * 1973 US Data Encryption Standard developed from lucifer– cracked in 1997 * 1974 Triple DES to increase security * 1976 – Diffie-Hellman key exchange - idea of public and private key encryption. Prior to this was the idea of using commutative encryption to achieve a similar effect. * 1977 - RSA – asymmetric public key. It works by multiplying 2 large prime numbers together (abs. massive). This is the public key, and they can’t work out what they original numbers are because just given the resulting number, it takes years to work out. Named for initials of creators. The algorithm is quite slow – generally used purely to send a symmetric key securely. This was the first public key cipher. The idea had been made by DH, but there was no one-way function they could use. Eventually they invented the one-way problem of factorising large prime numbers. * 1983 – Skipjack cipher (block cipher) and the clipper chip – a chip for encryption promoted by the US NSA, that had a back door, that allowed they government to break the code. * 1985 ElGamal encryption – based on Diffie-Hellman * 1985 elliptic-curve cryptography * 1987 RC4 - stream cipher * 1990 IDEA – international data encryption algorithm * 1991 PGP – pretty good privacy – other uses of codes by individuals – telegram/signal * 1991 – DSA – digital signature algorithm – based off public key encryption. You encrypt it in reverse, encrypting it with the private key, which proves it was encrypted by the person with the private key that corresponds to the public key they have released, and so can be used to verify identities. * 1993 Blowfish – symmetric key block cipher – AES and twofish preferred for modern applications * Mid 1990s – public key infrastructure discoveries by GCHQ made public * 1996 - CAST5 (CAST-128) – symmetric key block cipher * 1997 - AES developed * 1997 - MARS – block cipher – IBM’s submission to AES * 1998 – SHACAL -2 – 256 bit cipher – for NESSIE project * 1998 Twofish – AES submission – better than blowfish * 1998 Serpent – AES submission * 1998 HC-128 – stream cipher – fast? * 2000 – Camelia – symmetric key block cipher – as good as AES * 2000 – DES replaced by AES. A competition was held for companies and individuals to submit ciphers and the most effective one would become the new standard. It was the Rijndael block cipher, developed by 2 Belgian cryptographers. It is symmetric key.   Interesting stories relating to modern encryption   * In America, the FBI recovered the phone of a suspect in a shooting. The FBI could not break Apple’s encryption used to protect the data on the phone, so they got the Department of Justice to send an order to Apple that they break the encryption. Apple refused, and demanded that they retract the order. They said that they did not support terrorism, but that if they followed the order, it would set a dangerous precedent. They refused to create such a software that could decrypt the phone, knowing that it would not just be used once, and there would always be the possibility that a criminal could obtain it. They said the only way for such software to be secure was to never create it. In the end, the FBI used 3rd party software to unlock the phone, and Apple was never forced to cooperate. * The clipper chip. Law enforcement realised that terrorists could use phones to communicate securely as the encryption was unbreakable – this was a big problem. So they decided to suggest key escrow. Ordinarily 2 keys are generated in encryption – one for the sender, and one for the receiver, but in this case a 3rd would be generated for the government, held in escrow. If they obtained a warrant, they could use this key to listen in on the communications. On Feb. 4 the White House announced its approval of the Clipper chip, a chip that would be used in phones for their encryption, but that would incorporate key escrow technology. Ultimately, people refused to buy phones using the clipper chip, and the government couldn’t make them. The only people who bought phones using it where, in the end, government departments. * The government is attempting to reduce end-to-end encryption in messaging services (like Facebook) using the Online Safety Bill. Nobody, not even the people who own the messaging service can see the messages with end-to-end encryption, but the government maintains that this allows people to send messages about crimes, without being intercepted. Some companies maintained that they would not cooperate even if the bill was passed in full. Some also said that they would leave the UK in the event it was passed. The bill will apply to any service that has users in the UK, or targets the UK as a market, even if it is not based in the country. Breaking the rules could mean organizations are fined up to 10% of global annual turnover or £18 million (US$22 million), whichever is higher.   Methods of Breaking Codes   * Known plaintext attack * Brute force attack – try every key * Depth attack * Statistical attack – frequency analysis   *Possible quotes for part 1 and the sources they are from:*  “In the 1970s, academic papers on encryption were classified. Cryptographic devices were subject to export controls and rated as munitions, particularly in the US. Encryption was regarded as a matter of national security.”   “With end-to-end encryption, the context of every exchange - a text message, a video chat, a voice call, an emoji reaction - is intelligible only to the sender and the recipient. If a hacker or a government agency intercepts an exchange, the intruder sees a nonsensical snarl of letters and numbers.”  (End to end encryption is where the text is encrypted before it leaves the sender, and decrypted only when it has been received by the recipient.)  “Quantum computing (and its exceptional power) is in its infancy but may break asymmetric cryptographic algorithms.  The result?  Experts foresee that RSA 2048 can be broken by 2035.”  “On the other hand, zero-knowledge proofs, while a cryptographic concept, are a more specific tool within that larger cryptography toolbox.  They are a method by which one party can prove to another that they know a specific piece of information without revealing any details about the information itself.”  <https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption> This source is produced by an IT company that works in encryption, so their expertise in this field could make this more reliable. However, this page is not important to their business so they may not have put too much effort into it, making it less reliable.  “If someone tells you, “I don’t need security. I have no secrets, nothing to hide,” respond by saying, “OK, let me see your medical files. How about your paycheck, bank statements, investment portfolio and credit card bills?”  “In addition to keeping secrets, cryptography can add security to the process of authenticating people’s identity. [….] If attackers want to pose as someone else, it’s not a matter simply of guessing a password. Attackers must also solve an intractable mathematical problem.”  “All computer crypto operates with keys. Why is a key necessary? Why not create an algorithm that doesn’t need a key? […] if attackers can understand the algorithm they can recover secret data simply by executing the algorithm. […] It might seem that the solution is to keep the algorithm secret, but that approach has several problems. First, attackers always crack the algorithm […]. Unless you are a cryptography expert and develop your own algorithms, you also must trust the company that wrote your algorithm never to reveal it deliberately or accidentally.”  RSA Security’s Official Guide to Cryptography This source is likely to be reliable as it was written by RSA press, working for RSA Security, the company that developed the most popular public key encryption mechanism (RSA) that is used in virtually all modern computers.  “A zero-knowledge proof […] is a method by which one party (called the prover) can prove to another party (called the verifier ) that they know value x, without having to convey or prove any information except for the fact that they really know the value x, without actually providing value x or leaking any extra, nonessential information.”  “Quantum-based cryptography is also inherently resistant to known quantum attacks, as well as attacks from traditional binary computers.”  “How long would it take an attacker to try 50 billion keys? Three years? Three days? Three minutes? Suppose you want to keep your secret safe for at least three years, but it takes an attack only three minutes to try 50 billion values. Then what do you do? You choose a bigger range.”  Cryptography Apocalypse – R Grimes (the author) has worked in cyber security for over 20 years and has many certifications, so this source is likely to be reliable.  “During the Middle Ages, cryptography started to progress. All of the Western European governments used cryptography in one form or another, and codes started to become more popular. The earliest ciphers involved only vowel substitution (leaving consonants unchanged).”  “By 1860 large codes were in common use for diplomatic communications, and cipher systems had become a rarity for this application. Cipher systems prevailed, however, for military communications except for high-command communications because of the difficulty of protecting codebooks from capture or compromise in the field.”  “The invention of telegraph and radio pushed forward the development of cryptographic protection of telecommunications: the speed and the volumes of data traffic became considerable and more vulnerable to interception and decryption. The radio espionage was closely following the development of new telecommunications technologies, but paradoxically, the telegraphic and radio exchange of information was mainly in clear or done in plain ciphers. It was not until the 20th century mathematical theory and computer science have both been applied to cryptanalysis.”  <https://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html> – this appears to be a form of blog, suggesting that it is written by someone who may not have any qualifications or expertise. This makes it less reliable.  “Due to recent developments in software and hardware, some consumer-level encryption products are now so powerful that law enforcement officials say they can't crack them, even with massive supercomputers.”  “Given the current power of computers, a 56-bit key is considered crackable; a 128-bit key isn't – at least not without an enormous amount of effort.  Until 1996, the U.S. government considered anything stronger than 40-bit encryption a "munition" and its export, therefore, was illegal. The government now allows the export of 56-bit encryption, with some restrictions – but 128-bit cryptography is emerging as the new digital standard.”  “Finally, if Dan's bosses – or the government – insist that there be some way for them to decode his encrypted data and messages in case he gets hit by a truck or appears to be engaging in illegal activity, there are a few basic options. Dan can be forced to turn over a "spare" copy of his secret key to a third party, either private or governmental, who will only allow it to be used under certain circumstances. Or, along the lines of the government's failed "Clipper Chip" initiative, Dan can be told to use only encryption products that automatically create a master key, held in reserve by a third party. Those options are known as "key recovery" or "key escrow."”  “Before 1991, the government and large companies were the only real users of encryption technology. That began to change when programmer Philip Zimmermann released free software called Pretty Good Privacy, which can encode ordinary e-mail.  Its domestic use was never challenged. But when PGP turned up in other countries, the Department of Justice launched a three-year criminal investigation of Zimmermann. PGP used 128-bit encoding keys at a time when U.S. export laws allowed only 40-bit encryption to cross the borders. Anything stronger was classified a munition, just like guns and warheads.  No charges were filed against Zimmermann. But the case dramatically highlighted the sharply differing views toward encryption technology.”  <https://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm> - The Washington post is quite highly regarded, and so may be somewhat reliable. However, it is a news website and so may lack technical expertise.  “The increasing value of knowledge, and in modern times, data, has spurred the evolution of cryptography. The oldest known cryptography preserved religious or commercial knowledge and was then influenced by the need for secure military communication. The next drastic changes came when secure commercial and private communication became a general necessity. Since the 1980s, computers and the internet have increasingly come to dominate our lives. Thus, in the Information Age, all communication is best encrypted, regardless of it being between humans, machines, or humans and machines.”  [About the scytale] “This was the first time the concept of a common key, seen even today in modern cryptographic technologies, was used for both encryption and decryption.”  “Several factors pushed encryption towards the mainstream. The most important of these was the invention of the World Wide Web in 1989 and the widespread use of computers. Both industrial-commercial and personal communication had to be protected. For example, financial services were some of the first to require secure electronic transactions. Other businesses wanted to secure their digitally stored trade secrets. Finally, individuals wanted to rest assured that their online communication was secure. Today virtually all digital communication is, or should be, encrypted.”  “RSA introduced the concept of a public-private key pair for encryption. The public key is used to encrypt data, which can then only be decrypted with the corresponding private key. Although the two keys are mathematically related, calculating the private key from the public is extremely complex and time-consuming, thanks to a mathematical problem called prime factorization. The RSA algorithm also laid down the foundations for modern authentication methods as the use of a private-public key pair was perfect for identifying if the sender is who he says he is and also ensured better safety in messaging.”  <https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/> - run by an IT Cloud company which uses encryption in their products. However, this page is not important to their business so it may not be as reliable as other sites.  [Regarding ancient substitution ciphers like Caesar] “It is easy to see that such ciphers depend on the secrecy of the system and not on the encryption key. Once the system is known, these encrypted messages can easily be decrypted.”  “The secrecy of your message should always depend on the secrecy of the key, and not on the secrecy of the encryption system. (This is known as Kerckhoffs's principle.)”  <https://www.redhat.com/en/blog/brief-history-cryptography> This site is run by a software company that provides open source software, a subsidiary of IBM.  <https://www.researchgate.net/publication/353999208_CRYPTOGRAPHY_FROM_THE_ANCIENT_HISTORY_TO_NOW_IT'S_APPLICATIONS_AND_A_NEW_COMPLETE_NUMERICAL_MODEL> - journal - abandoned due to generally poor grammar  “By everyone's estimation, the invention by Diffie and Hellman was a  pivotal moment in network security, a crucial component of public  privacy, and also an elegant and simple mathematical solution.  In essence, Diffie and Hellman developed a way for two people to set up  a secure communication channel without ever meeting. Encryption was  well-understood at the time, but no one had a very good idea of how to  handle the keys that are used to keep the data secret. The keys are  long numbers that act to scramble the data. Anyone with a copy of the  key can read the data, but the message remains secret to those without  a copy.  Before the invention, people had to either agree to a key in advance or  have some trusted courier carry a copy between them. Today, banks  still have this problem distributing PIN numbers to the people who use  their ATMs. The banks send the cards and the PIN numbers in different  envelopes to minimize the possibility that someone could steal both.  Diffie and Hellman found a way to use fairly simple arithmetic with big  numbers to let two people agree upon a key. The crucial detail was that  anyone eavesdropping on the conversation would not be able to pick up a  copy of the key by listening to the negotiation.”  “To find a key, Alice chooses a random number "a" and Bob chooses a  random number "b." They also agree on some value of "g" in advance.  Alice ships g^a [that is, g raised to the power a, as in  2^3=8] to Bob and Bob ships g^b to Alice. Alice computes  (g^b)^a and Bob computes (g^a)^b. These are equal according to  the basic rules of algebra and they can serve as the key.  The system can't be broken because the arithmetic occurs in a "finite  field." That is, after each arithmetic operation, the result is divided  by some prime number, "p," and only the remainder is kept. This is  often indicated by appending "mod p" to the equation. Surprisingly, all  of the basic rules of arithmetic and algebra still apply. Some  operations, however, are harder. No one knows an efficient way to take  g and g^a and find a. This is known as taking the "discrete log," and  the fact that no one has described an easy way to do it means that the  link is secure. No eavesdropper can listen in and take apart the (g^a)  or the (g^b) to discover a or b.”  <https://www.ics.uci.edu/~ics54/doc/security/pkhistory.html> - Part of the Donald Bren school of information and computer sciences, so likely to be factual and accurate.  [Regarding PGP public key encryption] “What this PGP version did was to allow people to have two distinct keys, one that was kept secret and one that would be given away. If a message was encrypted with one it can only be decrypted with the other. This is one of the basic elements in key encryption and is also used in conjunction with an algorithm to determine how the possible communication will be encrypted and decrypted. It also allowed two new freedoms,  To “sign” a message, guaranteeing to a recipient that in come from them. This is accomplished by encrypting the message with a private key, which only the sender knows. The only code that can decrypt the message is the public key, which the recipients know belongs to the sender.”  <https://www.giac.org/paper/gsec/1555/history-encryption/102877> - GIAC is a cyber security body that trains and certifies people. The writer will likely have a certification and might be more reliable – note, sometimes poor grammar  <https://www.axel.org/2021/05/28/history-of-encryption/> - could not find any good quotes  “The first to actually record methods of cryptanalysis […] were the Arabs. […] It was not until 1412, with the publication of the fourteen volume work *Subh al-a ‘sha* that the complete documentation of the Arabic knowledge of cryptography appeared. One of the important features of this work was that it contained the first systematic explanation of cryptanalysis in recorded history.  <https://cubo.ufro.cl/ojs/index.php/cubo/article/view/1645/1496> – from a mathematical journal and so should be reliable.  On specific encryptions:  Scytale  “One of the oldest cryptography tools was a Spartan scytale. It is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Spartans and Greeks, in general, are told to have used this cipher to communicate during military campaigns.”  <http://ozscience.com/technology/a-scytale-cryptography-of-the-ancient-sparta/> - privately funded initiative for the advancement of science and technology in Australia.  Vignere  “The weakness of the vigenere cipher lies in its short key and is repeated, so there is a key loop in encrypting messages, this is used by cryptanalysts using the Kasiski method to know the key length so it can solve this algorithm.”  “the amount of work can measure the level and strength of a cipher needed to break the ciphertext data into plaintext without knowing the key used in the encryption process. The more work needed, the longer it takes to break the ciphertext into plaintext without knowing the key to a cipher. This means that the stronger the cipher is, the more secure the cipher is used to protect the message to be kept confidential. This study describes how the strength of the cipher in the vigenere cipher algorithm and RESEARCH ARTICLE OPEN ACCESS International Journal of Computer Techniques -– Volume 6 Issue 6,November 2019 ISSN :2394-2231 http://www.ijctjournal.org Page 2 the modification of the vigenere cipher to the Kasiski method attack by knowing the key length used in the ciphertext (cipher attack).” – not just relevant to Vigenere  Prior to the Kasiski method, the Vigenere was considered unbreakable“possible to decrypt the ciphertext itself. The Kasiski method helps find the length of the key by using advantages such as the English plaintext which contains not only letter repetition but also looping of pairs of letters or triple letters such as "TH", "THE", and so on. This letter repetition makes it possible to produce repetitive cryptograms”  <https://arxiv.org/abs/1912.04519>  “Vigenere cipher, being poly-alphabetic cipher was one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher”  “Encryption in Vigenere cipher is fast but the decryption process is slow”  <https://www.researchgate.net/profile/Yumnam-Kirani/publication/235741546_Generalization_of_Vigenere_cipher/links/0fcfd51304111ad522000000/Generalization-of-Vigenere-cipher.pdf> – from the journal of engineering and applied sciences and so is likely to be reliable and accurate.  Enigma  “In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress.  The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt a message.”  “Around December 1932 Marian Rejewski, a Polish mathematician and cryptologist at the Polish Cipher Bureau, used the theory of permutations, and flaws in the German military-message encipherment procedures, to break message keys of the plugboard Enigma machine.”  <https://profilpelajar.com/article/Enigma_machine>  One time pad  “There has been quite a bit discussion and some experts argue that one-time pad is no longer a system for today's needs, that it is impractical and creates enormous key distribution problems. They say that current computer algorithms provide enough security and public key schemes solve the problem of key distribution. This paper explains why reality is very different and why one-time pad will eventually be the only future.”  “The system was invented in 1917 and it is mathematically unbreakable. There is no way to crack it with current or future computer power, simply because it is mathematically impossible. The downside is that the rules of one-time use create a cumbersome key distribution with associated problems.”  “A good old quote of NSA’s David Boak says it all. "The ‘approved’ systems have simply been shown to adequately resist whatever kinds of cryptomathematical attacks we, with our finite resources and brains, have been able to think up. We are by no means certain that the [opponent] equivalent can do no better".”  “Information theory taught us that only a truly random key, as long as the message, will enable encryption that resist cryptanalysis. Any key that is shorter than the message, regardless how random it is, will eventually provide the clear and unique solution to breaking the message. This is a mathematical fact. In the end, only perfectly secure encryption will survive the evolution of cryptography. Just as classical pencil-and-paper ciphers were rendered useless with the advent of the computer, so will current computer based crypto algorithms become victim to the evolution of technology.”  <https://www.ciphermachinesandcryptology.com/papers/is_one_time_pad_history.pdf>  DES  On private key encryption : “The key is the secret to breaking the ciphertext; if there exists a really secure method of communicating the key, why isn’t that method used to communicate the message in the first place?”  “Public-key cryptosystems when used for data encryption are extremely computationally demanding and thereby slower than the symmetric ones but provide arbitrarily high levels of security and do not require an initial private-key exchange”  <https://www.researchgate.net/profile/Kefa-Rabah-2/publication/45949430_Theory_and_Implementation_of_Data_Encryption_Standard_A_Review/links/02e7e51af7fd2a3cbb000000/Theory-and-Implementation-of-Data-Encryption-Standard-A-Review.pdf> – in the Information Technology Journal and so likely be accurate and reliable.  “Fast and hard, that is all that cryptographers have ever wanted: a system that encrypts quickly but is essentially impossible to break. With their reliance on elementary number theory, public-key systems have captured mathematicians’ imagination”  “Conventional wisdom holds that in order to defy easy decryption, a cryptographic algorithm should produce seeming chaos; that is, ciphertext should look and test random. In theory an eavesdropper should not be able to determine any significant information from an intercepted ciphertext.”  “Cryptographers design their algorithms to resist the following list of increasingly aggressive attacks: • ciphertext-only: The adversary has access to the encrypted communications;  • known-plaintext: the adversary has some plaintext and its corresponding ciphertext;  • chosen-text: the adversary chooses the plaintext to be encrypted, or the adversary picks the ciphertext to be decrypted (chosen ciphertext), or the adversary chooses the plaintext to be encrypted depending on ciphertext received from previous requests (adaptive chosen plaintext).  Chosen-text attacks are largely used to simplify analysis of cryptosystems, but because of such devices as “smart cards” (credit card-sized objects equipped with a small processor), such attacks can occur in practice.”  “Fifty years ago Claude Shannon observed that the fundamental techniques for encryption are confusion— obscuring the relationship between the plaintext and the ciphertext—and diffusion—spreading the change throughout the ciphertext. Substitution is the simplest type of confusion, and permutation is the the simplest method of diffusion.”  <https://www.ams.org/journals/notices/200003/fea-landau.pdf?trk=200003fea-landau&cat=collection> – American mathematical society journal article.  RSA  “RSA implemented two important ideas:  1. Public-key encryption. This idea omits the need for a “courier” to deliver keys to recipients over another secure channel before transmitting the originally-intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.  2. Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn’t just come from there (authentication). This is done using the sender’s decryption key, and the signature can later be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny having signed the message.  This is not only useful for electronic mail, but for other electronic transactions and transmissions, such as fund transfers. The security of the RSA algorithm has so far been validated, since no known attempts to break it have yet been successful, mostly due to the difficulty of factoring large numbers n = pq, where p and q are large prime numbers.”  “RSA is slower than certain other symmetric cryptosystems. RSA is, in fact, commonly used to securely transmit the keys for another less secure, but faster algorithm.”  <https://pdfdirectory.com/pdf/0702-the-rsa-algorithm.pdf>  elliptic curve  [Desirable parts of a communications system]  “Confidentiality  Only an authorized recipient should be able to extract the contents of the encoded data, in part or whole.  Integrity  The recipient should be able to establish if the message has been altered during transmission.  Authentication  The recipient should be able to identify the sender, and verify that the purported sender actually sent the message.  Non-Repudiation  The sender should not be able to deny sending the message, if he actually did send it.  Anti-replay  The message should not be allowed to be sent to multiple recipients, without the sender’s knowledge.  Proof of Delivery  The sender should be able to prove that the recipient received the message.”  “Public key cryptosystems rely on the existence of a trapdoor function, which makes decoding possible given the knowledge of the private key corresponding to the public key for encryption”  “The ECC is based on the Elliptic Curve Discrete Logarithm problem, which is a known NP-Hard problem.”  “The main advantage ECC has over RSA is that the basic operation in ECC is point addition (see Appendix B), which is known to be computationally very expensive. This is one of the reasons why it is very unlikely that a general sub-exponential attack on ECC will be discovered in the near future, though ECC has a few attacks on a few particular classes of curves. These curves can be readily distinguished and can be avoided. On the other hand, RSA already has a known sub-exponential attack which works in general. Thus, to maintain the same degree of security, in view of rising computing power, the number of bits required in the RSA generated key pair will rise much faster than in the ECC generated key pair”  <https://dl.acm.org/doi/pdf/10.1145/1386853.1378356>  AES  On the use of padding in block ciphers  “In order to use the Rijndael algorithm the data must be a multiple of the block size, since all blocks need to be complete. When the data is not a multiple of the block size some form of padding must be used. Padding is when extra bits are added to the original data. One forms of padding includes adding the same bytes until the desired size is reached. Another option is padding with all zeros and having the last byte represent the number of zeros. Padding with null characters or random characters are also forms of padding that can be used.”  “Decryption is simple after understanding the encryption process. It is basically just the inverse. The algorithm was designed for all the steps to be invertible so decryption is basically like doing everything backwards.”  <https://www2.rivier.edu/journal/roaj-fall-2010/j455-selent-aes.pdf> - An academic journal, so it should be reliable.  More general sources  <https://journal.ijresm.com/index.php/ijresm/article/view/1556> - abandoned due to poor grammar, too short and mostly just a list of facts and descriptions that can be found elsewhere.  The black chamber website    “Cryptography is a way of secure transmission and storage of data such that only the party for whom it is intended can read and others cannot. Cryptanalysis is the art of breaking codes, cipher text and cryptosystems without knowing the key or algorithm. Cryptology includes the study of both cryptography and cryptanalysis. Encryption is the process of converting plaintext to cipher text with the help of suitable schemes, algorithms and key. Thus the message encrypted can only be decrypted by the intended recipient with the help of corresponding decryption algorithms and key.”  “Since the earliest of times, humans have been interested in keeping certain sensitive information that they possess out of the reach of others for whom it isn‟t intended”  “About 1467 AD, an Italian mathematician, Leon Battista Alberti developed polyalphabetic ciphers and was given the title, “Father of Western Cryptology”.”  “World War II Cryptography This period marked the use of more and more mechanical and electromechanical cipher machines. Major advancements in cipher design and cryptanalysis were made. Between 1920- 1930, a cipher machine called the Enigma rotor machine was invented by Arthur Scherbius which was used by the German Army.”  “The most famous ones are the transposition ciphers and the substitution ciphers. The transposition ciphers work by rearranging the alphabets or changing the order of the alphabets appearing in a word. For example, „first‟ becomes „ifrts‟, whereas substitution ciphers [1] works by replacing letters or group of letters with other letters or group of letters.”  <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b861e8de6f3fa5e7aba25d06daa5fa7d45f54f93>  “The earliest form of cryptography was the simple writing of a message, as most people could not read (New World, 2007).“  “In fact, the very word cryptography comes from the Greek words kryptos and graphein, which mean hidden and writing, respectively (Pawlan, 1998).”  “The Caesar Shift Cipher is an example of a Monoalphabetic Cipher. It is easy to see why this method of encryption is simple to break. All a person has to do is to go down the alphabet, juxtapositioning the start of the alphabet to each succeeding letter. At each iteration, the message is decrypted to see if it makes sense. When it does appear as a readable message, the code has been broken. Another way to break Monoalphabetic ciphers is by the use of what is known as frequency analysis, attributed to the Arabs circa 1000 C.E. (New World, 2007). This method utilizes the idea that certain letters, in English the letter "e," for instance, are repeated more often than others. Armed with this knowledge, a person could go over a message and look for the repeated use, or frequency of use, of a particular letter and try to substitute known frequently used letters (Taylor, 2002).”  <http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography> - academic journal.  “…the development of codes can be viewed as an evolutionary struggle. A code is constantly under attack from codebreakers. When the codebreakers have developed a new weapon that reveals a code’s weakness, then the code is no longer useful. It either becomes extinct or evolves into a new stronger code.”  “To render a message unintelligible, it is scrambled according to a particular protocol, which is agreed beforehand between the sender and the intended recipient.”  “Cryptography itself can be divide into two branches, known as transposition and substitution. In transposition, the letters of the message are rearranged, effectively generating an anagram.” P11  “This form of secret writing is called a substitution cipher because each letter in the plaintext(the message before encryption) is substituted for a different letter to produce the ciphertext (the message after encryption)” P13  “Julius Caesar. He simply replaces each letter in the alphabet with the letter that is three places further down the alphabet.” P14  “Each distinct cipher can be considered in terms of a general encrypting method, known as the algorithm, and a key which specifies the exact details of a particular encryption”  “1883 Auguste Kerckhoffs von Nieuwenhof in La Cryptographie Militaire “Kerchoffs’ Principle: the security of a cryptosystem must not depend on keeping secret the crypt-algorithm. The security depends only on keeping secret the key”  “In addition to keeping the key secret, a secure cipher system must also have a wide range of potential keys. For example if the sender uses the Caesar shift cipher to encrypt a message, then encryption is relatively weak because there are only twenty-five potential keys.”  “From the enemy’s point of view, even if the message is intercepted and the algorithm is known, there is still the horrendous task of checking all possible keys.”  “…it would take roughly a billion times the lifetime of the universe to check all of them [the keys] and decipher the message”  “This simplicity and strength meant that the substitution cipher dominated the art of secret writing throughout the first millennium AD. Codemakers had evolved a system for guaranteeing secure communication, so there was no need for further development”  “…establish the frequency of each letter of the alphabet. In English, e is the most common letter […]. Next, examine the ciphertext in question, and work out the frequency of each letter. If the most common letter in the ciphertext is, for example j, then it would seem likely that this is a substitute for e.” – frequency analysis  “Technically, a code is defined as substitution at the level of words or phrases, whereas a cipher is defined as substitution at the level of letters.”  Simon Singh – The Cracking Codebook – highly regarded author likely to be a reliable source  Part 2 - What is quantum computing and how are quantum computers superior to modern computers?  Introducing the quantum world   * What does quantum mean? * Quantum principles * Quantum physics   + Superposition   + Entanglement – faster than light   + No-cloning   What is quantum computing?   * When did it begin – Feynmann 1981 speech * Advances * Types of quantum computer   How are quantum computers superior to modern computers   * Advantages of superposition in qubits. * The many-universes theory – many Q-computers working in parallel between dimensions. * Problems with quantum computers   + Why they don’t work that well now   + Why there are some things they will never be able to do.   *Possible quotes for part 2 and the sources they are from:*  “The word “quantum” needs a little demystifying to be used safely. It does nothing more than establish that we are dealing with “quanta”, the tiny packets of energy and matter that are the building blocks of reality. A quantum is usually a very small speck of something, a uniform building block”  “At this quantum level, it is possible to link particles together so completely that the linked objects […] become, to all intents and purposes, part of the same thing. […] Make a change to one particle, and that change is instantly reflected in the other(s) - however far apart they might be”  On locality, defied by entanglement “If we want to act upon something that isn’t directly connect to us […] we need to get something from us to the object we wish to act upon”  “This need for travel – travel that takes time is what locality is about. It says you cant act on a remote object without that intervention”  On Quantum computers  “Conventional computers don’t understand randomness – they are deterministic […] but true randomness is an essential if a computer is to accurately reflect the quantum world.”  “a quantum computer could do anything a normal computer cold do, and, crucially, that it could make use of the peculiarities of the quantum world to provide parallel operations for which there could be no equivalent in a normal computer.  Brian Clegg – the God Effect – he has written multiple other books on science and phenomena, and is likely to be somewhat reliable. He has a background in physics.  “Richard Feynman observed in the early 1980s [Feynman 1982] that certain quantum mechanical effects cannot be simulated efficiently on a classical computer. This observation led to speculation that perhaps computation in general could be done more efficiently if it made use of these quantum effects.”  “Classically, the time it takes to do certain computations can be decreased by using parallel processors. To achieve an exponential decrease in time requires an exponential increase in the number of processors, and hence an exponential increase in the amount of physical space needed. However, in quantum systems the amount of parallelism increases exponentially with the size of the system. Thus, an exponential increase in parallelism requires only a linear increase in the amount of physical space needed. This effect is called quantum parallelism [Deutsch and Jozsa 1992]. There is a catch, and a big catch at that. While a quantum system can perform massive parallel computation, access to the results of the computation is restricted. Accessing the results is equivalent to making a measurement, which disturbs the quantum state. This problem makes the situation, on the face of it, seem even worse than the classical situation; we can only read the result of one parallel thread, and because measurement is probabilistic, we cannot even choose which one we get.”  <https://dl.acm.org/doi/pdf/10.1145/367701.367709> - History and introduction to quantum comp.  “It has been estimated that every two years for the past 50 years computers have become twice as fast while their components have become twice as small [Lloyd, 1995]. If progress continues at this rate future computer circuits will be based on nanotechnology”  “Quantum computers cannot compute a function that is not Turing-computable, but they do give new methods of computation for many classes of problem.”  “Instead, the orbit of electrons is best described as a wave (Figure 1). There are several different types of orbit, depending on the angular momentum and energy level. An electron ‘jumps’ orbit from an orbit with low energy level to an orbit with high energy level by absorbing energy (e.g. a photon). The term ‘quantum’ signifies that there can be no in-between states or orbits. The jumps are discrete, and the energy levels can be roughly characterised as the number of cycles an electron has to go through while orbiting the nucleus at that energy level”  <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c5a58aa3662b027a1d5ae38f460ddc0edf16e2d0> – This is written by a member of the computing Department at Exeter university and so should be somewhat reliable.  “Superposition is a principle that states while we do not know the state of an object at a given time, it is possible that it is in all states simultaneously, as long as we do not look at it to check its state. The way that energy and mass become correlated to interact with each other regardless of distance is called entanglement.“  <https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/#:~:text=Quantum%20computing%20focuses%20on%20the,entanglement%20to%20perform%20data%20operations>.  “While interestingly, they are not universally faster than classical computers, they do perform specific types of calculations faster. Each operation may not be faster, however the number of operations necessary to arrive at a result using particular algorithms is exponentially small. “  “The power of these qubits is their inherent ability to scale exponentially so that a two-qubit machine allows for four calculations simultaneously, a three-qubit machine allows for eight calculations, and a four-qubit machine performs 16 simultaneous calculations.”  <https://www.edn.com/the-basics-of-quantum-computing-a-tutorial/> - This is an electronics industry website  “The commercial annealing-based quantum computer D-Wave 2000Q has about 2000 qubits (Gibney, 2017). The quantum-annealing-based quantum computer is not a universal computer but designed to solve optimization problems.” – Annealers are a special type of quantum computer that are much easier to build, but only work on a few problems.  “In this section, a photon is used as an example of a qubit for the sake of ease. The polarization (i.e., the geometric orientation of the photon) represents one-bit information. A horizontally polarized photon represents classical bit 0, and a vertically polarized photon represents bit 1. In Figure 1, photons are fired at the emitter and going through the Filter-V, which allows only vertically polarized photons to go through. We assume only a single photon goes into Polarization Beam Splitter (PBS) at a time to make the example simpler. PBS transmits vertically polarized photons (measured at the detector DV) while the PBS deflects horizontally polarized photons (measured at the detector DH). Thus, all photons will be measured at DV in Figure 1. |𝜓⟩ = 𝛼|0⟩ + 𝛽|1⟩,{𝛼, 𝛽 ∈ ℂ} (1) |𝜓1 ⟩ ⊗ |𝜓2 ⟩ = [𝜓1,0 , 𝜓1,1 ] 𝑇 ⊗ [𝜓2,0 , 𝜓2,1 ] 𝑇 = [𝜓1,0𝜓2,0 ,𝜓1,0𝜓2,1 ,𝜓1,1𝜓2,0 , 𝜓1,1𝜓2,1 ] 𝑇 (3) Quantum Computing: Principles and Applications Kanamori & Yoo ©International Information Management Association, Inc. 2020 47 ISSN: 1941-6679-On-line Copy . Figure 1: All photons are detected at DV If a filter that only transmits diagonally polarized photons called “Filter-45°”, however, is placed between Filter-V and PBS (Figure 2), a vertically or horizontally polarized photon is found at each detector with the probability of ½.” – every photon is in a superposition  <https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1410&context=jitim> – Part of the Journal of International Technology and Information Management and so should be reliable.  “The quantum annealer has been successfully developed by Canadian company D-Wave, but it is difficult to tell whether it actually has any real “quantumness” thus far. Google added credibility to this notion in December 2015, when it revealed tests showing that its D-Wave quantum computer was 3,600 times faster than a supercomputer at solving specific, complex problems.  Expert opinion, however, is still sceptical on these claims. Such criticisms also shed light on the major limitation of quantum annealers, which is that they may only be engineered to solve very specific optimization problems, and have limited general practicality.”  “However, building such a device ends up posing a number of important technical challenges. Quantum particles turn out to be quite fickle, and the smallest interference from light or sound can create errors in the computing process.”  <https://www.visualcapitalist.com/three-types-quantum-computers/> - this is a website on business opportunities and investment trends which has no particular expertise in science or quantum computing and could therefore be less reliable.  “Symmetric key quantum resistance  This refers to the inherent ability of traditional symmetric key encryption and authentication algorithms to resist quantum attacks. […] symmetric ciphers are not susceptible to Shor’s algorithm, and Grover’s algorithm cuts their protection in half. So, in a sense, symmetric key ciphers are already quantum resistant, as long as their key sizes are of sufficient size to fight off Grover’s algorithm attacks.”  Cryptography Apocalypse – R Grimes (the author) has worked in cyber security for over 20 years and has many certifications, so this source is likely to be reliable.  “They [qubits] can exist in a superposition of states, meaning they can represent multiple values at the same time, and they can also become entangled with each other, allowing for parallel computation. This makes quantum computing potentially much faster than classical computing for certain types of problems, such as factorization and database searching.”  “The biggest quantum computing challenge, arguably, is qubit decoherence. Qubits are extremely sensitive to their environment, and even small disturbances can cause them to lose their quantum properties, a phenomenon known as decoherence. The struggle to master decoherence may require new materials, new computational techniques and deep exploration of various  quantum approaches. It’s not just the hardware that’s challenging for quantum computing. Quantum algorithms are also much more complex than classical algorithms and require developers to approach computational problems in original ways.”  “Quantum computers are extremely sensitive to noise and errors caused by interactions with their environment. This can cause errors to accumulate and degrade the quality of computation. Developing reliable error correction techniques is therefore essential for building practical quantum computers.”  “While quantum computers have shown impressive performance for some tasks, they are still relatively small compared to classical computers. Scaling up quantum computers to hundreds or thousands of qubits while maintaining high levels of coherence and low error rates remains a major challenge.”  “Quantum computers won’t replace classical computers; they will serve as complementary technology. Developing efficient and reliable methods for transferring data between classical and quantum computers is essential for practical applications.”  – e.g., when factoring a number into 2 primes, the Q-computer will hold both primes in superposition, but only one can be read, so a classical computer will use the first prime to work out the other  <https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/>  Part 3 - How quantum computers break existing encryption and what can be done about it?  Breaking codes with quantum computers  How are quantum computers able to break codes so quickly?  What sort of codes can be broken quickly?   * Shor’s algorithm breaking certain public key cryptography mechanisms * Grover’s algorithm, reducing the security of every key size of symmetric encryption to ½ (really it square roots the efficiency, reducing time taken by ½)   What sort of defences are there/codes that can’t be broken, and why can’t they be broken?  Quantum-proof classical encryption   * An exponential speed up is insufficient * Or, the problem is intractable   Quantum key exchange   * The no-cloning principle * This makes public-key encryption redundant. * Limitations – cost of setting up the infrastructure and range limitations   *Possible quotes for part 3 and the sources they are from:*  “In 1994, Peter Shor discovered an algorithm to factor numbers in bounded probability polynomial time on a quantum computer, along with another to compute discreet logarithms. The factoring algorithm uses a reduction of the factoring problem to the problem of finding the period of a function, and it uses the quantum Fourier transform in finding the period. Quantum parallelism makes it possible to work with superpositions of all possible inputs, which is the key to the increased power of this algorithm when compared to classical algorithms.”  “Shor’s algorithms have obvious and potentially catastrophic implications for the field of cryptography. Many cryptosystems, including the popular RSA cryptosystem, depend for their security on the assumption that factoring large numbers is difficult; others depend on the difficulty of computing discrete logarithms. The discovery of this polynomial-time quantum factoring algorithm means that anyone with a quantum computer could easily crack RSA and many other cryptosystems, and possibly much more” – only exponential-time and above problems are considered to be hard  <https://digitalcommons.dartmouth.edu/cgi/viewcontent.cgi?article=1022&context=senior_theses>  “Shor's algorithm brings an exponential speed-up for solving the factoring, discrete logarithm (DLP) and elliptic-curve discrete logarithm (ECDLP) problems that are widely used in cryptographic applications.”  <https://www.sciencedirect.com/science/article/abs/pii/S1361372317300519>  On QKD - “If anyone attempts to intercept a polarised photon, it will affect the polarisation and make it impossible to consistently recover the key that is encoded in the stream of qubits”, so the key will not be used.  “QKD is unlikely to be a universal answer to the risk posed by quantum computers for three reasons: (1) The security relies upon quantum mechanical principles and only recently has work been publicly reported on developing formal proof that QKD is semantically secure; [38]  (2) QKD requires an expensive infrastructure;  (3) QKD can operate over relatively short distances: the longest to date being approximately 150 km although some reports suggest over 300 km has now been achieved”  “The mathematical problems that are most actively being investigated are  (1) Lattice-based cryptography  (2) Multivariate-based cryptography  (3) Hash-based signatures  (4) Code-based cryptography  (5) Supersingular elliptic curves-based cryptography.”  <https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1226650> – this is an article in the Journal of Cyber Security Technology and so this source is likely to be relatively reliable.  “Quantum computers endanger the principal goal of all secure and authentic communication because they can do computations at a rate that classical computers cannot. Cryptography is a critical component of today's advanced communication systems. The security of emails, passwords, or financial transactions has the objectives of confidentiality and integrity [11]. Cryptography makes sure that only parties that have exchanged keys can read the encrypted message, thereby preserving the purpose of secure communication. Consequently, quantum computers can break the cryptographic keys quickly, using brute force alone, by calculating or searching for all secret keys. Quantum computers are a double-edged sword and eavesdroppers are likely to exploit quantum algorithms to optimize certain tasks that threaten secure communication. One such algorithm, published by Peter Shor, helps quantum machines find the prime factors of integers incredibly fast. Another algorithm, by Lov Grover, helps quantum computers iterate through possible permutations at a faster rate.”  “Unlike RSA, rather than multiplying primes, lattice-based encryption schemes involve multiplying matrices. The shortest vector problem (SVP) is an NPhard problem, and its objective is to find the smallest non-zero vector in the lattice. Lattice-based cryptosystems' security relies on coordinates within a lattice system that are difficult to solve [18]. Currently, existing algorithms for solving SVP take exponential time in the dimension of the lattice. Since quantum computers are not quick at solving problems with multiple solutions, it also takes exponential time on a quantum computer.”  <https://www.mecs-press.org/ijwmt/ijwmt-v12-n5/IJWMT-V12-N5-2.pdf>    “First, there is a time lag between when a cryptosystem is proven broken and when it becomes patched or replaced. A classic example is the Heartbleed vulnerability (CVE-2014-0160) in OpenSSL where 300,000 servers were still vulnerable two months after its revelation. If a breach is expected or possible, it is preferable to transition away from the vulnerable technology before it is compromised. Second, it would be unknown which data was secure. As will be discussed in this paper, most quantum-based attacks could be interceptions, meaning that it is possible that a message between two legitimate parties could be read without alerting either one. This would cause massive uncertainty for all encrypted message, because there would be no way to guarantee that data is transferred without interception. Third, when the capable quantum technology arrives, the algorithms for breaking current cryptographic standards will have already been developed. Mathematicians are already devising quantum algorithms for breaching some of the world’s most used encryption methods, most notably the Rivest-Shamir-Adleman cryptosystem (RSA) and elliptic curve cryptography (ECC).”  “The current recommendation of a 2048-bit RSA number would require 4096 qubits to break.”  “A subset of post-quantum cryptography is quantum key distribution and quantum cryptography: cryptography that relies on quantum mechanics much like quantum computing attacks do. The message transfer begins by one party sending a stream of photons to another; the state and characteristics of each proton are used to generate the key. If the photons are examined at any point between the sender and the receiver, the receiver’s detector will notice an error rate in the photon values and alert the two parties. If the key is generated correctly, the key is used to encrypt and send the message.38 Because silent interception is not possible, and the key is completely random, the quantum key is virtually unbreakable and it ”is considered the most powerful data encryption scheme ever developed.”39 While there presently are issues with implementation that prevent it from being uncrackable, this form of encryption is ideal because it is theoretically unbreakable and its security does not depend on the state of existing technology.”  <https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf>  “quantum tamper-detection in the case of encryption schemes: in this work, a classical message is encrypted into a quantum ciphertext such that, at decryption time, the receiver will detect if an adversary could have information about the plaintext when the key is revealed. We note that classical information alone cannot produce such encryption schemes, since it is always possible to perfectly copy ciphertexts.”  “Quantum Key Recycling. The concept of quantum key recycling is a precursor to the QKD protocol, developed by Bennett, Brassard, and Breidbart [BBB14] (the manuscript was prepared in 1982 but only published recently). According to this protocol, it is possible to encrypt a classical message into a quantum state, such 1We thank an anonymous reviewer for this suggestion. 5 that information-theoretic security is assured, but in addition, a tamper detection mechanism would allow the one-time pad key to be re-used in the case that no eavesdropping is detected.”  <https://arxiv.org/pdf/1903.00130.pdf>  “The security of most public key cryptosystems depends on the difficulty of solving some mathematical problem, such as factoring large numbers or computing discrete logarithms in finite field or elliptic curve groups. The best known solutions to these problems run in exponential (or sub-exponential) time, making it infeasible for attackers to break the schemes.”  “Existing quantum-resistant schemes generally have several limitations. Compared with traditional RSA, finite field, and elliptic curve discrete logarithm schemes, all quantum-resistant schemes have either larger public keys, larger ciphertexts/signatures, or slower runtime. Many quantum-resistant schemes are also based on mathematical problems that are, from a cryptographic perspective, quite new, and thus have received comparably less cryptanalysis.”  <https://link.springer.com/chapter/10.1007/978-3-319-69453-5_2> – this is from an international conference on areas of cryptography, and so likely to be accurate and reliable.  “When a user visits a website starting with https, the user’s computer uses “Transport Layer Security” (TLS) to connect securely to the web server. TLS combines a sequence of cryptographic operations to ensure that no third party can understand what is being sent (confidentiality), that no third party can modify the messages without being detected (integrity), and that no third party can impersonate one of the communicating parties (authenticity).”  “These algorithms, when applied to widely deployed public-key sizes for RSA and ECC, require billions of operations on thousands of logical qubits. Fault-tolerant attacks seem likely to require trillions of operations on millions of physical qubits. Perhaps quantum computing will encounter a fundamental obstacle that prevents it from ever scaling successfully to such sizes. However, no such obstacles have been identified. Prudent risk management requires defending against the possibility that these attacks will be successful.”  “Many more cryptographic systems are affected by an algorithm that Grover [18] introduced in 1996. This algorithm is also the foundation for most, although not all, of the positive applications that have been identified for quantum computing. Grover originally described his algorithm as searching an unordered database of size N using √ N quantum queries. This begs the question of why the database creator did not simply put the database into order, allowing it to be searched using O(log N) queries. A closer look at the details of Grover’s algorithm also raises difficult questions regarding the physical cost of quantum database queries.”  <https://eprint.iacr.org/2017/314.pdf> – this source could be useful for part 2 as well  “Symmetric algorithms offer efficient processing for confidentiality and integrity, but key management (i.e., establishing and maintaining secrets known only to the communicating parties) poses a challenge. Symmetric algorithms offer weak proofs of origin since either party to an exchange can calculate the transformation. Asymmetric algorithms generally require more processing operations and time than are practical for providing confidentiality protection for more than very small volumes of data. However, these algorithms are practical for cryptographic key establishment and digital signature processes. In the case of public-key cryptography, one of the keys in a pair can be made public, and distribution of private keys is not needed. Asymmetric key algorithms can be used to establish pairwise keys and authenticate an entity and/or data source in many-to-many communications without demanding a secret channel for key distribution. As a result, most cryptographic entity or data source authentication and key establishment functions use public-key cryptography”  “it is likely that future post-quantum cryptographic standards will specify multiple algorithms for different applications because of differing implementation constraints (e.g., sensitivity to large signature size or large keys). For example, the signature or key size might not be a problem for some applications but be unacceptable in others. In such cases, NIST standards could recognize the need for different applications to deploy different algorithms. On the other hand, existing protocols might need to be modified to handle larger signatures or key sizes (e.g., using message segmentation).”  <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf> – This is a government paper and so should be almost totally reliable, especially as it is from the Institute of Standards and Technology.  “The origin of security of QKD can be traced back to some fundamental principles of quantum physics. One can argue for instance that any action, by which Eve extracts some information out of quantum states, is a generalized form of measurement; and a well-known tenet of quantum physics says that measurement in general modifies the state of the measured system. Alternatively, one may think that Eve’s goal is to have a perfect copy of the state that Alice sends to Bob; this is however forbidden by the no-cloning theorem (Wootters and Zurek, 1982), which states that one cannot duplicate an unknown quantum state while keeping the original intact.”  “The fact that security can be based on general principles of physics suggests the possibility of unconditional security, i.e. the possibility of guaranteeing security without imposing any restriction on the power of the eavesdropper (more on this notion in Sec. II.C.1). Indeed, at the moment of writing, unconditional security has been proved for several QKD protocols.”  <https://arxiv.org/pdf/0802.4155.pdf>  Other resources:  Books:   * The Cracking Codebook (Simon Singh) * A shortcut through time - the path to the quantum computer (George Johnson) * The God Effect (Brian Clegg) * The Quantum Universe: everything that can happen does happen (Brian Cox, Jeff Forshaw) * Computing with Quantum Cats (John Gribbin) * Cryptography apocalypse (Roger A Grimes) * RSA Security’s Official Guide to Cryptography (Steve Burnett, Stephen Paine).   Timeline (planning includes acquiring quotes)   * Finish planning history of encryption by 25/5/23 * Finish planning quantum computing/physics by 10/6/23 * Finish planning the threat quantum computers pose and how it can be mitigated by 20/6/23 * **26/6/23 Submit planning review** * Start writing history of encryption by 10/7/23 * Finish writing history of encryption by 25/7/23 * Start writing quantum computing/physics by 10/8/23 * Finish writing quantum computing/physics by 3/9/23 * **15/9/23 Submit mid-project review** * Start writing threats and mitigation by 20/9/23 * Finish writing threats and mitigation by 3/10/23 * **5/10/23 Presentation** * **13/10/23 Submit end project review, summary and reflection** |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | The candidate could add more detail regarding their resources. Otherwise the candidate appears very well prepared. |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor** | I will add more details to my resources regarding their clarity and reliability. |

**Supervisor’s Signature:** **Date:**

**MID-PROJECT REVIEW**

**Candidate’s Full Name:** **City & Guilds Registration Number:**

**To be completed by the candidate**

This page records your outline plan half-way through your work.

|  |  |
| --- | --- |
| **Outline what has been successful and what has been less successful. Have any additions and/or changes been made to your original plan?** | I have had some problems to overcome during my writing. Initially in section one my word count was far too large and so I decided to use this as a draft. In my second attempt I managed to reduce it to a reasonable level but it was not as easy as I had hoped. My ability to find journal articles to research my topic has been improved thanks to my supervisor showing us how to use Google Scholar however many articles are behind a pay wall and as you can only see a small part of them I am still somewhat limited by what I can access.  I am generally happy with how my essay is proceeding. I am pleased with my use of time management and have kept my EPQ on track. I found my time line and Gantt chart useful in helping with this. I decided to add a separate document to evaluate my sources based on input from my supervisor in the Planning Review. I have also been using a work log to evaluate my progress which I think will be useful when I need to write my summary and evaluation. I feel that I have managed to keep section two from becoming too difficult to understand despite the complexity of the quantum phenomena I am discussing and am pleased that I have been able to keep this section within a reasonable word count in comparison to the first draft of section one.  I have made some changes to my original plan. I decided to add my aims and what I hope to accomplish into my introduction as I have found that these points are typical of an introduction to a research paper and that they are necessary to make my intentions clear to the reader. I have also decided to include quantum interference in section two as it is relevant to quantum computing, both in how we interact with computers and in why they are so difficult to build.  I am seriously considering making a slight change to my title. I am thinking of changing it from “How has encryption evolved and what does the future hold for it in the age of quantum computing?” to “How has encryption evolved and can it survive in the age of quantum computing?” This is to make it less vague and easier to argue and draw conclusions on rather than being an open ended question. I am keeping it very similar though so that I will not have to alter the first two sections of my essay. |
| **Outline your planned steps to complete your project** | I intend to complete section three of my essay (The quantum computer: what threat does it pose and how can it be mitigated?) and write the conclusion, drawing everything together and answering the question my title poses. I will then have to write my evaluation and summary of how my work progressed, the problems I faced and how I overcame them. Finally, I will create a presentation (using PowerPoint software) on my EPQ to present to my classmates. |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | My supervisor thought that “How has encryption evolved and can it survive in the age of quantum computing?” was a preferable title. He agreed that I should change the title as it would not affect the sections I have already written and would make writing my conclusion easier. I also asked for clarification on whether an abstract was required or not. My supervisor was able to tell me that it is not necessary and so I have deleted my draft abstract. Finally, I asked for advice on the timeline going forward to ensure my presentation and evaluation timings were correct. |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor at this stage** | I have decided to change my title to “How has encryption evolved and can it survive in the age of quantum computing?” for my project. I was initially concerned that it might not be possible to change the title at this late stage in the project so I am pleased that my supervisor agreed that this was the right course of action. This will be useful when writing the third section of my essay and my conclusion.  I have also deleted my draft abstract as it is not required. I am aware that research papers include an abstract so I was glad to have clarification from my supervisor on this matter. |

**Supervisor’s Signature:**  **Date:**

**END-OF-PROJECT REVIEW**

**Candidate’s Full Name:**  **City & Guilds Registration Number:**

**To be completed by the candidate**

This page records the (near) completion of your project product.

|  |  |
| --- | --- |
| **Outline the successes, failures, additions and/or changes you made as you followed the plan in your mid-project review** | Following on from my mid-project review, I am very pleased that I have been able to update my title to be clearer and less vague. I am also satisfied with my completion of section three and my conclusion, which was made easier by my improved title. I felt I gave an effective and concise overview of the threat quantum computing poses, and how it can be dealt with, as well as summing up my thoughts on everything in the conclusion. Throughout section 3 and the conclusion, I had learned from my previous mistakes and I am happy that I had much greater success in keeping these sections succinct and with the word count. I had overlooked referencing during my mid project review, however I have now completed a great deal of research into the different referencing systems (I am using IEEE) and have completed my referencing list. Finally, I have also started my presentation on schedule and have created the individual slides and the layout of the PowerPoint. Going forward, I will be working on completing this PowerPoint and the summary/reflection. |
| **Outline any additional advice or comments that you received from your supervisor during this stage** | I spoke to my supervisor about referencing systems as I was unsure if there was a particular system that we had to use. He said that we were able to use any system that we liked as long as it was consistent.  I also asked him whether I should just have a reference list or have a bibliography. I had written a reference list but then realised that this meant a large number of sources that I had read, but did not quote, would be excluded. I then wondered if I should do a bibliography instead but didn’t know if this would be compatible with my referencing system. My supervisor told me that it was possible to do both a reference list and a bibliography. |
| **Outline changes, clarifications or additions you have made as a result of your discussion with your supervisor in this final stage** | I researched different referencing systems as I thought this information could be useful. As we were able to use any referencing system I chose to use IEEE. I decided to use this system because it was the example system we were shown by our supervisor and it is also the system used in computer science by the university I hope to attend. It also helps to keep my word count down as only a number is required at the end of a quote rather than a name and date.  I have also added a bibliography to my reference list as my supervisor said that it was possible to do so. This meant I was able to include all the sources I had used and not just those that I had quoted from. |

**Supervisor’s Signature:** **Date:**

**SUMMARY**

**Candidate’s Full name:**  **City & Guilds Registration Number:**

**To be completed by the candidate**

This page provides you with an overview of your project.

|  |
| --- |
| **Provide detail of your project title, aims, main content, what you did to achieve your objectives, project findings and conclusions.** |
| Title  For my project I decided on the title “How has encryption evolved and can it survive in the age of quantum computing?”.  Aims  I wanted to examine how encryption has evolved to reach the point it is at today. I also wanted to explore how quantum computers function, and explain how they are superior to modern computers. Finally I planned to analyse the threat quantum computers pose to current cryptographic infrastructure and investigated how the threat quantum computers pose could be mitigated.  Research  My initial research involved reading books relevant to the subject and looking at websites and journal articles about my topic. I bought several books from ebay and used Google Scholar to find articles. I then used these sources to find some key quotes that could be used in my essay.  Main content  My essay initially focuses on the evolution of cryptography from ancient Egypt up to encryption today, looking specifically at important changes or new forms of cryptography. I initially intended to cover some less important developments, but the word count meant I could include only the most significant ones that improved cryptography. Following this, I wrote about quantum mechanics concentrating on those mechanics that quantum computers make use of to give them their inherent capabilities. I particularly look at entanglement and superposition as well as the no-cloning theorem, which relates to my third section. However, I also look at the history of quantum computing, a quantum computer’s advantages and why they are so difficult to build to give context. In my final section I investigate the ways in which quantum computers render encryption vulnerable – the specific algorithms used to break the encryption. However, I also go on to talk about the ways in which the threat of these algorithms can be mitigated so that encryption can remain strong and secure.  I found that there were two specific ways in which quantum computing renders current encryption vulnerable. Grover’s algorithm weakens current symmetric encryption, and Shor’s algorithm makes most common asymmetric encryption insecure. Shor’s algorithm presents a much greater threat, but there are ways to mitigate both forms of attack. There is a simple way to defend against Grover’s algorithm – increase the size of the key for the encryption algorithm. This effectively negates the speedup the algorithm offers. However, Shor’s algorithm requires entirely new algorithms and mechanisms to defend against it. I discovered two key ways to defend against Shor’s algorithm which I explore in the third section – quantum intractable encryption and quantum key distribution.  Project findings/conclusions  I came to the conclusion that public key encryption as it is now may not survive, as current asymmetric encryption is extremely vulnerable to quantum attacks. However, I believe it can evolve to use algorithms that are not vulnerable to Shor’s algorithm. Symmetric encryption would have to use increased key sizes to defend against attacks using Grover’s algorithm, but should otherwise survive as it is today. Therefore I believe encryption will survive in the age of quantum computing. |

**Candidate’s Signature:**  **Date:**

**PRESENTATION RECORD – PART A**

**Candidate’s Full Name:**  **City & Guilds Registration Number:**

**To be completed by the candidate**

This page records your presentation and its preparation.

|  |  |
| --- | --- |
| **How are you going to present your project?** | I am going to use PowerPoint to present my project. I intend to have between 15 and 20 slides covering reasons for doing an EPQ, aims and objectives, research, introduction, the three sections of my essay, conclusion, and my evaluation which will be split between skills, successes and lessons learned. I will end with any questions. |
| **Planned structure of your presentation (e.g. timing, audience, use of visual aids, slides, use of notes, etc.)** | I intend the presentation to take around 10 minutes and my audience will be my Cyber EPQ classmates and Supervisor. Alongside my Powerpoint I will have printed notes to prompt me.  The first third of my presentation will look at the work I did prior to my EPQ and the reasons I had for doing it. The next part focuses on the content of my essay and the final section will evaluate the project by looking at the skills I learned, what was successful and what I would do differently next time. |
| **Briefly list the main content of your presentation** | |  |  | | --- | --- | | Title | Content | | Title slide | Name and title | | Reasons for doing an EPQ | * University * New skills * Personal Interest * Course Modules * Previous Interest * Inspired by a Book | | Aims and Objectives | * Explore the evolution of cryptography. * Investigate how quantum computers function. * Explain how quantum computers are superior to modern computers. * Analyse the threat quantum computers pose to existing cryptographic infrastructure. * Examine how the threat quantum computers pose can be mitigated. | | Research | List of my 5 most useful sources. | | Introduction | * What is cryptography/   encryption?   * Why is encryption important? * Could quantum computing render encryption obsolete? | | A Brief History of Cryptography | * Ancient Cryptography   + Scytale   + Caesar Cipher   + Vigenère Cipher * Cryptography in the World Wars   + Enigma   + One Time Pad * Modern Cryptography   + DES   + AES   + RSA | | Quantum Mechanics and the Quantum Computer | * What is a quantum computer? * Origins of quantum computing * What are the different types of quantum computer?   + Quantum Annealer   + Analogue Quantum Computer   + Universal Quantum Computer * Why are quantum computers so difficult to build? | | The Threat Quantum Computing poses and how it can be mitigated | * The threat quantum computers pose   + Grover’s Algorithm   + Shor’s Algorithm * Defending against quantum attacks   + Increasing key sizes   + Quantum intractable encryption   + Quantum key distribution | | Conclusion | * Encryption has reached the point where it is almost impossible to break. * Quantum computers have started to develop from concepts into powerful machines. * Once quantum computers reach their peak, they will be able to break most of the asymmetric encryption we use today. * However, there are ways we can defend against the threat   + Increased key sizes   + Quantum intractable encryption   + Quantum key distribution | | Skills Developed | * Independent working * Time management * ICT skills * Communication skills * Referencing skills * Planning and organisational skills | | What was Successful | * Time management * Planning * Structure * Making complex topics accessible * Title change * Engagement | | Lessons learned and what I’d do differently next time | * Difficulties with the word limit. * Problems finding free research material. * More specific title. * Don’t choose too broad a topic. * Manage your time. * Shorter plan. | | Any Questions? | Any Questions? | |
| **Outline changes, clarifications or additions you made as a result of rehearsal and/or discussion with your supervisor** | The first time I rehearsed my presentation it took over 30 minutes to complete. This was obviously too long so I had to look at ways to cut it down considerably. I decided to remove the ‘Research’ slide as I hadn’t done any first hand research so I didn’t feel it contributed significantly.  The Brief History of Cryptography was particularly long so I decided to list the Scytale, Caesar cipher and Vigenère cipher but only talk about the Scytale in more detail.  I also decided to remove the parts on the origins of quantum computing and why quantum computers are so difficult to build. Explaining decoherence and error correction was quite time consuming and I felt that these parts were less necessary to an overall understanding of my project.  This reduced my presentation time but I still needed to compress it further. I had been talking around each topic to make it more interesting and detailed but realised I would need to pare this back to the bare minimum to try to keep within the time limit. By doing all these things I managed to reduce the time down to around 10 minutes. |

**Candidate’s Signature:**  **Date:**

**PRESENTATION RECORD – PART B**

**Candidate’s Full Name:**  **City & Guilds Registration Number:**

**To be completed by the supervisor**

Record and comment below on the delivery of the presentation

**Supervisor’s record / comments**

|  |  |
| --- | --- |
| **The nature of the audience (include numbers of staff, students and others present)** |  |
|  |
|  |
|  |
| **The nature of the presentation (include use of notes, use of display items, and use of presentation software)** |  |
|  |
|  |
|  |
| **Comment on the content and delivery of the presentation** |  |
|  |
|  |
|  |
| **Comment on the response of the candidate to questions that demonstrated understanding and grasp of the project and/or its productions (give examples where appropriate)** |  |
|  |
|  |
|  |
| **Outline the nature of any additional evidence that the candidate might add (e.g. speaker notes, hand-outs, presentation slides, recordings)** |  |
|  |
|  |
|  |
| **Proposed date and format of presentation** |  |
|  |
|  |
|  |

**Supervisor’s Signature:**  **Date:**

**REFLECTION**

**Candidate’s Full Name:** **City & Guilds Registration Number**

**To be completed by the candidate**

This page records your own evaluation when you have completed your project product and given your presentation.

**Briefly summarise the main learning aims you achieved when completing your project. You might include:**

* New knowledge, skills or expertise that you enjoyed or found valuable
* Strengths and weaknesses of your project
* A consideration of your planning and organisation
* Changes you would make if you carried out a similar project again
* Advice you would give to others undertaking such a project
* Own personal aspirations for further education and career development

|  |
| --- |
| **Knowledge and skills that I gained**  Completing my EPQ has allowed me to carry out a project outside of the curriculum with minimal teacher input. This has enabled me to feel confident researching, planning, writing and evaluating an independent project over a long period of time.  This project has helped me develop my time management skills by using a Gantt chart and time-line so that I was able to keep on track. I have also learned about researching useful sources for a project, for example by using Google Scholar and have been able to evaluate them for quality. I have investigated different referencing systems such as Harvard and Chicago and decided that IEEE would be the most useful for my essay. There were several reasons for this such as my supervisor demonstrating this system, it being used at the universities I am applying to and it only using numbers in the in-text citations which helped with my word count.  In addition to this my supervisor taught the class a number of other useful ICT skills including showing us how to use special characters to search for sources more effectively as well as showing us how to set up a document in the cloud using OneDrive so that we could access it at home and at school. He also showed us how to automatically format a document in word to add features such as a title page and table of contents, and automatic referencing in the IEEE style. I feel these skills will be very useful if I have to undertake a similar project at university.  I have also tried to improve my communication skills by asking my supervisor important questions. I am not very good at asking for advice or help and prefer to try to work things out for myself. I have found his feedback valuable, for example, when I was unsure whether to use a reference list or a bibliography. I had written a reference list but then realised that this meant a large number of sources that I had read but did not quote would be excluded. I then wondered if I should do a bibliography instead however my supervisor said that I could use both which solved my problem.  Planning and organisational skills are very important to be able to complete an EPQ successfully. I found the production log very helpful in planning my essay and the regular reviews helped to keep me focussed. My Gantt chart and time line as previously mentioned were also useful in this regard. Alongside my project I have also completed a work log which has kept track of the skills I have been developing and evaluated my progress. This has enabled me to appreciate the knowledge I have been gaining and look back on how far I have come.  **Strengths and weaknesses of my project**  **Strengths**  Throughout my project I believe I was able to use good time management to keep on track. I created a time-line and a Gantt chart to plan when I was going to complete each part of the project and used my work log to make sure that the project was on track. This meant I did not have to rush any parts of the project and was able to take the time to review and improve each part of my essay.  I was also able to plan extensively so that every part of my essay was covered in detail. I wanted to show that I had researched the topic in depth, so I gathered information on more of each section than I would actually be able to include within the word count to ensure I did not miss any important elements. As part of this, I obtained all my quotes and sources before writing the essay, which made writing the essay much easier as I did not have to repeatedly stop writing to gather quotes.  While I was planning my essay, I decided to split my project into three sections, and then further into subsections. This gave me strong structure for my essay, as well as allowing me to focus on each individual subsection, rather than becoming overwhelmed by trying to write the whole essay. This also made it easier to use time management, as I could aim to get each smaller section done within a certain timeframe, rather than simply trying to get the whole essay finished at a certain time.  After struggling with the word count, I decided to use a glossary in my EPQ. I was having to explain lots of terms in the essay that were using up a large number of words, without actually contributing much to the essay itself. Therefore, I included a glossary which allowed me to explain terms thoroughly without contributing to the word count. This meant I had more space in my essay to talk more in detail about the concepts the words related to. Ultimately, I was very pleased at the depth I was able to go to in the essay, despite the limited word count. In part two of my essay, which focuses on quantum mechanics and the quantum computer I describe some complex quantum phenomena. I am very happy that I was able to explain them in a concise and understandable way so that even someone without a very scientific background could understand what I am saying.  When choosing a cyber security related topic for the project I was struggling to decide between encryption and pen-testing. Eventually I chose encryption as I had some prior knowledge of the topic, which I thought would make researching it easier. I also decided to incorporate quantum computing into my topic as I knew almost nothing about it and hoped this would allow me to learn about something new and interesting not covered in the curriculum. Ultimately I found researching the subject very enjoyable, especially learning about the complex quantum phenomena which do not appear to conform to the classical laws of physics. I found that I engaged really well with the topic and felt this made the experience much more enjoyable and rewarding. I am confident that I have come away from the EPQ having learnt a great deal about encryption and quantum computing in addition to the many other useful skills I have developed.  Towards the end of my project, at the mid project review, I decided to change my title. This could have been a weakness as it was very late to be altering my title, but I feel that sticking with my old title would have been more of a weakness as it was too open-ended. This would have made drawing conclusions difficult and so I think that my new title was a strength. My new title was similar to the previous one, meaning that I did not have to rewrite the first and second sections of my essay, but was also much less vague, which made it much easier to write the third section and draw conclusions, answering the title question.    **Weaknesses**  Unfortunately, my extensive planning was a weakness as well as a strength. As my topic was large and I was not sure what I would cut, I planned for a bigger essay than the one I had to write, as I expected it would be easier to remove text than to add it in later and I wanted to show I had researched the subject in depth. However, when writing my essay I quickly passed the word count and I found it more difficult than I expected to reduce the word count. Even after I had removed all the text that did not contribute sufficiently to the essay, I was still over the word count, and I found it difficult to decide what parts of the essay I should keep and what I should discard.  Furthermore, I was not able to access some articles online because they required payment, or for you to be part of a university or institution, which I am not. This limited what sources I could obtain quotes from and reference, especially as these tended to be high quality journal articles. This also meant I had to spend longer trying to find good sources than I would have liked.    I was pleased with the PowerPoint element of my presentation but always find giving presentations difficult as I am autistic and talking in front of groups of people and eye contact are things I find quite difficult. I rehearsed the presentation in front of my family to help me prepare and found that it took 30 minutes to complete which was far too long. I then had to cut some parts out and greatly reduce the amount that I talked around each topic. I did however successfully manage to cut it down to just under 15 minutes.  **Changes I would make if I carried out the project again**  If I was to carry out the project again, I would limit my plan to a smaller length to help keep me within the word count, as I found that to be a severe problem. I would make sure to remove information I’m not going to include early on, so that when I come to write the essay I don’t have to pare it down nearly as much, as paring down the essay is more difficult than I anticipated.  Additionally, I changed my title in the mid-project review because it was too vague, which made it difficult to draw conclusions. Fortunately I had not yet written my third section and my conclusion, which were the only parts it affected, but if I was to do another similar project I would ideally want a clearer title from the start, as I do not have to worry about changing it later on.  **Advice for other students doing an EPQ**  Firstly, I would advise anyone undertaking an EPQ to draw up a time line or Gantt chart at the beginning of the project, and make an effort to stick to the timings, as the project as a whole requires a great deal of work. Rushing the project at the end will likely result in it being low quality, and I found that you need a long period over which to conduct research and gather quotes. I found it very useful having time to review each part of my essay after I had written it, to check for mistakes and to improve the quality of the section.  Furthermore, I would always advise you to plan heavily, but also to make sure that the amount of content you include in your plan reflects the length of the essay. If you include too little content, you will have to find more to say as you write the essay, which makes planning rather redundant, and will slow you down. However, if like me you write a plan that is too long, this can lead to your essay ending up far over the word count. Cutting the essay down to a reasonable size could prove very difficult as it did for me.  I would also recommend making sure your topic is not too broad, so that a 5000 word essay is sufficient to cover it. I chose both the history of encryption and quantum mechanics/computing, two very large subjects, and as such found it difficult to reduce my first section to fit the word count. I ended up having to remove large portions of the first section, and this meant I was not able to cover it as deeply as I would have liked. Fortunately, with quantum mechanics I was able to talk about only those phenomena that related to quantum computing, which helped keep that section concise.  Finally I would recommend that you practice speaking your presentation aloud and in front of other people if possible so you can see how it actually sounds – make sure you time it too.  Aspirations  When I finish sixth form, I am hoping to either attend university to study computer science or do a digital and technology solutions level 6 apprenticeship. Both of these are likely to involve elements of cyber security and probably an extended project, so I am sure that my EPQ will be of use. However, I am not exactly sure what direction I want to go in after further education and so I would like to keep my options open as much as possible. |

**Candidate’s Signature:**  **Date:**