To what extent is modern encryption secure and why have we reached this point?

In today's world, encryption underpins a multitude of the activities most of us conduct daily. These tasks include everything from checking emails to managing bank accounts and as such, the importance of strong encryption cannot be overstated. Here, I aim to explore the journey of development of cryptographic techniques from their first usage millennia ago to the modern day, where they are used by almost everybody, as opposed to only the few figures with power or wealth who could make use of cryptography during its initial stages. However, this only constitutes part of the story, another part being the ability to make and break newer, and increasingly advanced, ciphers, which can ultimately determine the balance of power.

Section One: The History of Cryptography

Primitive Ciphers

There were two main forms of early encryption: transposition and substitution[1]. Transposition is where the existing letters of a message are kept, but simply scrambled into different positions within the message in a reversible manner, while substitution is the replacement of existing letters in a message by new letters – usually more complex than transposition and the type that my research has been focused upon. One subset of this category is known as mono-substitution[2], in which each letter of a message is replaced by another letter, standardised across the whole text. An infamous example of this in use is from over two thousand years ago, during Caesar's Gallic Wars, when Roman letters were replaced with Greek ones, hence rendering the message unintelligible to those who did not know the substitution, or key, initially used[3]. There were a number of advantages to this system, though mainly its simplicity and its security to the unfamiliar cryptanalyst. With twenty-six letters in the English alphabet, by exhausting all mono-substitution cipher keys, we can mathematically obtain the potential number of cipher texts for any message if it contains at

[1] Singh, S. (1999). *The Code Book*. Fourth Estate. 4-24
[2] Ibid.
[3] Ibid.

least one of each letter: as there can be any arrangement of the 26 letters in the cipher compared to the plaintext, we have $26! = 4.03 \times 10^{26}$ potential ciphertexts for a single message – four hundred trillion trillion - unfathomably many if you were to attempt to decode the message by trying each possibility.

Based on this information, you might assume that this is a secure way to encrypt communications; however, it has some fundamental flaws. The Arab cryptanalyst Al-Kindi discovered a reasonably simple system of deciphering such messages in the ninth century CE[4]. It worked by using frequency analysis of letters found in the language and comparing this to the frequencies of letters observed in the cipher text and matching these appropriately using sensible assumptions, before improving the hypothesis gradually until you have a fully deciphered text. This might not always work, though, as a cryptographer may foresee the possibility of cryptanalysis being applied and modify the message itself to foil such attempts. For example, 'e' is the most common letter in English text at a frequency of 12.62%[5] and this is often used as a starting point for cryptanalysts, but in certain cases can be avoided entirely, such as in the lipogram *Gadsby*[6]. Nonetheless, a skilled and determined cryptanalyst would be able to break such a cipher eventually. This chain of events established the beginnings of the ever-continuing battle between cryptographers, trying to create ever more secure ciphers, and cryptanalysts, attempting to break each new iteration of these. It could be said that this continual desire for communications to be secure from one's perspective, but breakable from their opponent's perspective, is representative of the human nature to have some advantage over everyone else, be it allies or adversaries, which only served to propagate cryptographic advancement.

Invention of polyalphabetic encryption

The next main advancement by cryptographers was the creation of the Vigenère cipher, a form of polyalphabetic substitution. Its main strength is that a single letter can be encrypted into a range of different letters depending on the keyword and its length by using

[4] Al-Kadit, I. A. (1992). Origins of Cryptology: The Arab Contributions. Cryptologia, 107.
[5] Solso, R. L., & King, J. F. (1976). *Frequency and versatility of letters in the English Language*. Behavior Research Methods & Instrumentation, Vol. 8 (3), 283-286.
[6] Wright, E. V. (1939). *Gadsby*. Wetzel Publishing Co.

a Vigenère table, as shown in Fig. 1[7]. The keyword in use would be repeated multiple times over the plaintext, as many as needed to reach the end of it. Using the keyword letter above each letter of plaintext in correspondence with a Vigenère table provides each necessary letter of ciphertext, and repeating the same process with ciphertext gives each letter of plaintext. As you might imagine, this is significantly more difficult to reverse engineer than a mono-substitution cipher owing to the keyword's ability to change the encipherment of each individual letter throughout a message.

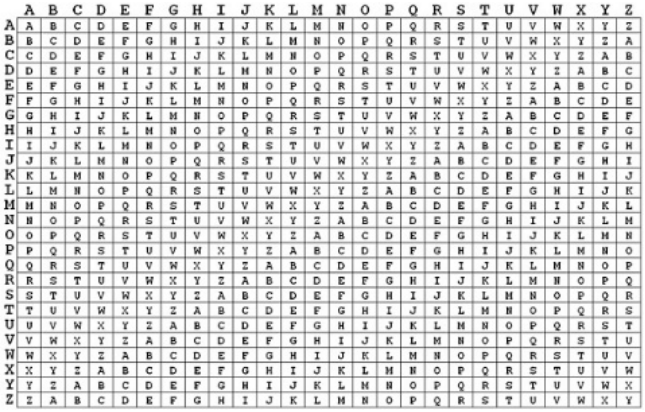

Fig. 1: A Vigenère Table

In the example shown in Figure 2, we can see that the letter 'A' has been encrypted into the letters 'P','N' and 'E' depending on its position relative to the keyword. This makes decryption a lot more difficult, and indeed the cipher was considered invulnerable until 1854, when British cryptographer Charles Babbage broke it[8]. A mathematical representation of the code is as follows[9]:

Figure 2: A Vigenère Encipherment

Keyword	PHONEPHONEPHONEP.
Plaintext	ASMALLQUICKESSAY.
Ciphertext	PZANPAXIVGZLGFEN.

$$Ci = E(Pi + Ki) \bmod 26$$

$$Pi = D(Ci - Ki) \bmod 26$$

Where C represents the cipher text, i the character index, P the plaintext character, K the key with E and D being the encryption and decryption functions respectively.

[7] Aliyu, A.-A. M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. *International Journal of Computer Applications 135, No. 11*, 46-50.
[8] Singh, S. (1999). *The Code Book*. Fourth Estate. 45-101.
[9] Aliyu, A.-A. M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. *International Journal of Computer Applications 135, No. 11*, 46-50.

It came into widespread use following the rise of monoalphabetic cryptanalysis, and due to its well-regarded security, was known as 'Le Chiffre Indéchiffrable' ('The Unbreakable Cipher' in English) – this became somewhat ironic after it was indeed broken. The way it was broken was remarkable and worked by exploiting the repeating key by first finding its length (looking for repeated phrases of cipher text and comparing them to common words, such as 'and' and 'the'), then using the length of the key to break down the ciphertext into 26 different Caesar ciphers which could then be solved using traditional cryptanalysis and logic[10]. This meant that shorter messages were much more secure and distractor letters became much more difficult to deal with, but these obstacles could still be overcome with a little ingenuity. Therefore, while a significant milestone in cryptography, 'Le Chiffre Indéchiffrable' was not yet the invincible one.

Codes at war

This next cipher is likely to be recognisable by name for most people who have at least a mild knowledge of World War Two – Enigma; this was used by Hitler's Nazi regime to conceal covert communications and wartime plans, usually between field agents. Invented in 1918, it was one of the first 'machines' to iterate over its component positions to encrypt text iteratively[11]. The Enigma machine, as it was known, had a keyboard and the ability to indicate output letters, with its primary strength, like the Vigenère cipher, being able to encode the same plaintext letter as many different things in the ciphertext – going above and beyond this by using electrical currents to create varying, yet reversible, polyalphabetic substitution ciphers. This worked by using a swappable plugboard matrix (wires connected to each input letter, for the military version anyway), rotors, the keyboard, and some additional internal circuitry[12]. Essentially, after each keystroke, one or more rotors would change their positions so that the next letter to be pressed would be much harder to decode in this complex machine – the keys were entered into Enigma by modifying the plugboard settings set, sent out by German headquarters regularly; there were 159 billion billion possible settings[13]. One

[10] Aliyu, A.-A. M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. *International Journal of Computer Applications 135, No. 11*, 46-50.
[11] Vacca, J. R. (2017). Computer and Information Security Handbook (Third Edition). Morgan Kaufmann. 36-37
[12] Singh, S. (1999). *The Code Book*. Fourth Estate. 155-157
[13] Ibid. 173

of its key strengths was the strength and speed of encryption/decryption, unlike the lengthy Vigenère cipher. Thus, a worthy, albeit even more deadly, successor.

To break it then, a great deal of hard work, imagination, and ingenuity was required. Originally, due to lack of want and funding in the British, American, and French code institutions, very little progress was made with French so-called cryptographers even declaring the challenge impossible in the pre-war years. Fortunately, the Polish vulnerability to German attack spurred on progress in the 1930s, exploiting Enigma's remaining flaws, such as repetition of certain keys, led primarily by Marian Rajewski[14]. By finding patterns in the encodings of successive letters, (using alternatively obtained cribs), he was able to find the links and therefore the scrambler part of the day key. Following this, Rajewski built 'bombe' machines capable of deducing the scrambler settings mechanically as the Germans modified Enigma sporadically. However, in 1938, Enigma was secured beyond Polish deciphering capabilities and budgets so following the country's invasion, work was shared with France and Britain to continue this invaluable mode of intelligence collection. With Alan Turing's revolutionary insights, such as how to construct a circuit of 3 Enigma machines so that the effect of the plugboard is nullified[15]. Using new devices inspired by Rajewski's bombes and advanced with Turing's originality, deciphering the new daily Enigma keys became far more regular, providing intelligence of such value that it is said to have shortened the war by several years. This feat of codebreaking ability was exceedingly impressive for the time and laid the framework for future developments in the field, especially thanks to Turing and Rajewski as individuals.

It should also be noted that, while the theory of these systems of cryptography is fairly sound, as detailed above, the secrecy of the key is paramount to a cipher's security. For example, if someone with a rudimentary knowledge of encipherment came across the key due to poor practice or carelessness, they would then be able to read any message encrypted with that key. To prevent, the key should be transmitted by 'non-interceptible means' between users[16]. This is why many of these ciphers are originally established in person, with the key memorised as to keep it secure – this sometimes also led to shorter

[14] Singh, S. (1999). *The Code Book*. Fourth Estate. 149-160, 170-175
[15] Ibid. 176
[16] Claude, S. Communication Theory of Secrecy Systems. *Bell System Technical Journal, 28*(4), 670

keys as a matter of ease for Vigenère ciphers, or distribution of one-time pads (containing all the keys for the near future in it) for something used in a similar way to Enigma.

Undoubtedly, the progression of cryptographic ciphers in the ways described above have been crucial in reaching the current state of encryption-omnipresent affairs, especially polyalphabetic ciphers. With the advancements made by Turing and others, such as Claude Shannon[17], during and after WWII, information theory became much more of a subject in its own right, as opposed to a branch of mathematics, with the art of cryptography being a major beneficiary. From this point on, ciphers continued becoming ever more secure, even overcoming some fundamental barriers, such as key distribution, by using new algorithms and far greater processing power. In some ways, the need for such orders of magnitude of encryption in modern society is disappointing as it is only necessitated by a grave lack of trust across wider human communities.

Section Two: Modern Cryptographic and Digital Security Means

The current standard and its mathematical theory

Compared to the methods that have been previously discussed, it might be easy to imagine that modern encryption is yet another iteration of substitution. However, unlike the jumps between Caesar to Vigenère or Vigenère to Enigma, modern systems use quite different concepts as to how data can be privately transmitted.

The primary new encryption method was known as 'Public Key Cryptography,' with its first, and most prevalent, implementation being RSA. Today, a variant of it is used almost universally in software packages for regular tasks, including key exchange, digital signatures, or encrypting small blocks of data[18]. Though given its near unbreakable nature, the underlying architecture has not changed much with technical modifications only, such as the minimum secure size of encryption units. Its primary advantage is the asymmetric approach to keys, thus circumventing the requirement for the previously discussed symmetric ciphers to have vulnerable key exchange methods (a symmetric cipher being one to use the same key for both encryption and decryption). The way it works is fairly simple from a conceptual view – each person has a private and a public key to use for the messages that they send and

[17] Ibid. 656
[18] Kessler, G. C. (2015). *An Overview of Cryptography.* Auerbach. P.6

receive with a one-way function used between these; for communication between two individuals, A and B, the process is as follows[19]:

- B chooses two large primes[20], p and q, with product $n = pq$.
- B then calculates $\varphi(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1)$ [21] and chooses a number e, coprime to $\varphi(pq)$; n and e then make up the public key, which A can then distribute.
    - For secure applications, n is usually greater than 10^{300}.
- B can then find the modular inverse, d, of e mod $\varphi(pq)$ such that d is the private key, which is not distributed.
- A, the sender can then use B's public key to encipher a message, which is then sent to B.
- B, the recipient, can then use their own public and private keys to decipher the message from A
- The same processes also work for A, or anybody for that matter, to receive and read an encrypted message from someone else.

The security of such a system and the sheer difficulty to break can, as it should, be explained mathematically. The real strength of RSA can be expressed in terms of key size (in bits), which is the number of digits in the number n, with greater key sizes being more secure[22]. Anything with a key size less than 512 bits (or $n < 10^{155}$) is no longer considered secure due to the ability of the most potent computers being able to factorise them. This whole idea operates on the idea of 'one-way' functions – an operation applied to two numbers that is relatively easy to do, but extremely difficult to undo. To demonstrate this, take the numbers 59 and 67, which are both prime, and multiply them – the result is easy to calculate by inspection, here being 3953. However, given a number with two prime factors and no other information, it is much more difficult to calculate its factors, with the length of time taken increasing exponentially with the length of the factors involved. For instance,

[19] Preetha, M., & Nithya, M. (2013, June). A Study and Performance Analysis of RSA Algorithm. *IJCSMS, 2*(6), 131-134.
[20] An integer greater than one with exactly two positive integer factors is to be considered prime.
[21] φ is the Euler totient function.
[22] IBM. (2021). *Size considerations for public and private keys*. Retrieved from IBM Documentation: https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys

while the multiplication from earlier was easy to compute, it is a very different exercise to factorise something that could even be smaller, such as 3403. Scaling this up to account for the computational strength of modern systems, IBM have calculated a table of standard key sizes that can be used for 'secure' RSA[23]:

Key Size	Relative Key Strength
512 bits	Low
1024 bits	Medium
2048 bits	High
4096 bits	Very high

Figure 3: RSA cryptography strength by key size

For most applications and encrypted messages used today, you can expect that the longer key sizes from this table will be the ones in use. The private key, therefore, being made of the all-important factors, is the only practical method that can be used to decode a message encrypted by the public key. As a mathematical technique, this is very elegant and the relative lateness of its discovery perhaps highlights the relative lack of research into pure mathematics in the second half of the 20th century. Nonetheless, mathematics prevailed to deliver a truly modern solution to an age old problem.

Related to this, it is also worth noting the origins of RSA encryption. For the most part, credit is given to Rivest, Shamir and Adleman (after whose initials it is aptly named) in 1977, though the British Government claims to have invented the idea beforehand[24]. According to the Government Communications Headquarters (GCHQ), the United Kingdom's signals intelligence agency, commissioned a classified investigation by James Ellis into solving the key-distribution problem. Ellis came to the same conclusion about the need for a one-way function, later found by GCHQ mathematician Clifford Cocks in 1973, thereby discovering a form of the RSA algorithm nearly four years earlier. However, due to their required compliance with the Official Secrets Act, his contributions went unknown until well after other people were recognised for 'discovering' the same ideas, as is the UK Government's cryptography modus operandi. To some extent, this must raise questions into how many inventions that can be used for the public good are classified and concealed by statutory

[23] Ibid.
[24] Singh, S. (1999). *The Code Book*. Fourth Estate. 281-292.

intelligence agencies, such as MI5, GCHQ, KGB (now GRU) or CIA, with no greater justification other than the guise of 'national security'. As such, a strong argument can be made as to require intelligence agencies to disclose at least what types of proprietary technology they may have. However, this would of course lead to potential detriment to national security, so a sensible balance would have to be struck.

Applications and deployment scenarios

In the real world though, RSA encryption is not used for everything. In fact, it is only really used for exchanging the key used to encrypt and decrypt files that have used a more traditional symmetric cipher to secure the contents[25]. Symmetric ciphers, excluding the problem around key exchange, are still very good at protecting data from anybody who does not have the key; modern-day ones could be thought of as infinitely more advanced versions of Enigma. This means that as long as the key can be distributed safely, using RSA, easier-to-compute symmetric ciphers can still be used in conjunction to manage longer communications that would take a long time on RSA. If systems like this are run well, abiding by protocols such as OAuth's 'best practices'[26] to ensure that a connected user can only ever access their own account and that they receive the correct keys to do this, then many common cyberattacks can be mitigated before a prospective user even begins to use a service. This is very important as real-life factors such as poor authentication flows are often the problem behind major cyberattacks, as opposed to the encryption technology underlying everything. Clearly then, humans are their own worst enemy when creating secure systems – far too often the human heuristic to 'take a shortcut' will overpower the rational process of building a fully consistent encryption system, and is at odds with the advanced theory which allows for theoretically unbreakable security.

Despite all of this, it would not be fair to mention only how encrypted services are secure or how they can be made more so, given that data leaks and hacks continue to happen. However, none of the mainstream attack vectors utilised by cybercriminals directly attack the encrypted RSA data tunnel – most instead exploiting vulnerabilities in each system

[25] Kessler, G. C. (2015). *An Overview of Cryptography*. Auerbach. 37-38
[26] IETF. (2023). *OAuth 2.0 Security Best Current Practice*. Retrieved from IETF Documentation: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics. Introduction

or server's architecture or with client-side access to the data[27]. For instance, attacks by 'Professionals', 'Hacktivists' or 'Nation States' are likely to include a precursor step of exploiting an operating system or server weakness before then leaking a database's information, stealing other data or planting information designed for sabotage. Note that all of these methods are being used against encryption endpoints, as any serious data is likely to have been encrypted using a key size of 4,096 bits, which is extremely difficult to break by brute force. In a sense, one could consider a lack of direct attack by hacking professionals as a testament to the security of the RSA public key cryptography paradigm.

The quantum potential

Although this may make public key cryptography seem impenetrable now, quantum computers offer a major threat to RSA-style encryption in the long term. The quantum computers of today do not pose a threat to the public key cryptography which is in widespread use. However, the theorised *Cryptographically Relevant Quantum Computer* (CQRC)[28], which can factorise the large numbers used for keys exceedingly quicker than current systems, potentially pose a major threat in the not-too-near future. Fortunately, there is one way to maintain secure key distribution amongst the quantum threat – 'Quantum Safe Cryptography'[29]. While this is one branch of cryptography, it is unlikely that a single algorithm could cover all applications as well as RSA key distribution does currently. Consequently, the National Institute for Standards and Technology of America has shortlisted several candidate algorithms for a new quantum standard such that by the time it becomes a real threat to consumers, the technology is already in place to prevent it. For example, IBM has developed a system that uses lattice-based digital signatures to help make this possible[30]. Essentially, while there is the possibility for quantum computers to pose a major threat, their expense and the defence mechanisms already being put in place restrict

[27] Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports 5 100167*. 5-7.
[28] National Cyber Security Centre. (2020, November 11). *Preparing for Quantum-Safe Cryptography*. Retrieved from NCSC GOV UK: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
[29] Ibid.
[30] IBM: Dames, Anne; Richuso, Emily. (2022, March 10). *What is Quantum-Safe Cryptography, and Why Do We Need It?* Retrieved from IBM: https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it

this level of interference away from amateur hackers and towards state-backed groups or research organisations, which is somewhat reassuring if anything.

It is certain, therefore, that in the short to medium term, for the vast majority of people, cybersecurity is sufficient to ensure reasonable privacy, although it requires correct implementation and care from both the consumers and providers. Hence, sensible cybercriminals would know where to focus their attack efforts and how to go about it undetected by law enforcement. Of course, this then begs the question of how cyberspace can be effectively policed by jurisdictional authorities, who face the same major obstructions to their monitoring as those whom they investigate.

Section Three: The Balance of Information

Human rights and privacy legislation

Information is one of the most important topics of the century, especially personal information, its gathering, its use, and its secure disposal by third parties – all digitally in the modern world, of course. Indeed, Article 12 of the Universal Declaration of Human Rights (UDHR) states the following:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*[31]

This certainly appears very absolute, yet its implementation into UK law includes an important caveat (Human Rights Act 1998 Article 12):

> 1) *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2) *There shall be no interference by a public authority with the exercise of this right* ***except*** *such as is in accordance with the law and is necessary in a democratic society* ***in the interests of national security, public***

[31] United Nations General Assembly. (1948). *The Universal Declaration of Human Rights (UDHR).* New York: United Nations General Assembly.

> ***safety or the economic well-being of the country**, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*[32]

Granted, it reads fairly ambiguously, but in practice, the investigative authority would obtain a court warrant to carry out the desired procedure so that evidence can be obtained, as long as this is within reason. Ordinarily, this is done with searches of tangible property, looking for any sort of incriminating document or else, but in the digital world the regulation and execution of state powers becomes much more difficult. Therefore, if an agency obtains access to records (using some of the methods described in section two) but decides to keep this secret, the public scrutiny by the judiciary is lost; hence this would lean into unlawfulness that is undiscoverable by anybody, except for whistleblowers.

The fight for privacy

For this level of legally guaranteed privacy to be sanctioned, there exist several reasonable arguments. Firstly, on the most fundamental level, the right to privacy establishes the '*realm of the personal by excluding it from public scrutiny*'[33], without which there is a high chance that people would live in fear or stress their whole lives. The consequence of this is generally poor governance as people's basic instincts dictate that constant monitoring is simply unjust – thus raising the chances of civil disobedience and poorer mental health across the populus. Moreover, the potential for data obtained by third parties to be misused is exceedingly high. Whether by companies, hackers or state-backed agencies, should a 'backdoor' exist for the authorities to use, there is simply no guarantee that they would not launch cases of arbitrary persecution; similarly, if a less moral organisation obtained access to people's information this way (perhaps from a disgruntled civil servant or by hacking) then the civil consequences would be disastrous, mass blackmail or extortion would likely occur[34]. Clearly then, it would seem as though the current legally defined level of privacy is justified.

[32] Parliament UK. (1998). *Human Rights Act.* Article 8. London: National Archives UK.
[33] Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & technology, 35(1)*, 3.
[34] Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & technology, 35(1)*, 3.

An issue for justice

However, going back to the provision in English Law mentioned earlier, there must be cases in which the 'national interest' takes precedent over individualistic privacy claims, such as when someone is under suspicion of the commission of a crime. The current specific law around this states a number of provisions around the obtention of telecommunication records, which was enacted by Parliament in 2016[35]. In short, there is an overwhelming requirement for 'senior' officers, who are in almost all cases to be independent of the inquiry itself, to authorise any access to telecommunications records as available from the relevant corporations; this is meant to happen for any sensible reason, such as for national security, preventing crime or disorder, economic well-being of the country, public safety and other similar factors. However, there are limited cases when these criteria can be relaxed, such as if there is imminent threat to life, the operation is so secret that knowledge of it must be at a minimum, or if the opportunity to obtain information so that it can be used effectively is highly limited[36]. Consequently, the restrictions for law enforcement and public authorities to obtain important data has a high chance of being rejected from a courtroom if there is even a slight impropriety – even if the truthfulness of the evidence itself is perfectly valid.

Moreover, these arguably bureaucratic obstacles in place, requiring senior officers to review every case rather than allowing investigations to progress as quickly as possible, have potentially exacerbated the rise of certain types of crime over the last decade. Taking fraud offences as an example (as use of technology is instrumental in its commission), in the year up to September 2014 there were 603,920 reported cases of fraud, whereas in the year up to December 2022 there were 3.7 million fraud offences[37]. This represents an increase of over 600% in less than 10 years for a crime that inflicts such damage on its victims and society in general. Yet, due to stringent restrictions on legitimate data collection, all in the name of 'privacy', it is very difficult for police to pre-emptively identify sources of cybercrime to tackle it effectively. Furthermore, greater collection of personal data, such as biometrics, a wide

[35] Parliament UK. (2016). *Investigatory Powers Act*. London: National Archives UK.
[36] Parliament UK. (2016). *Investigatory Powers Act*. London: National Archives UK. (63(3))
[37] Office for National Statistics. (2023, April 27). *Crime in England and Wales Statistical bulletins*. Retrieved from ONS (GOV UK): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/previousReleases

expansion of CCTV cameras and facial recognition would allow for more targeted policing and deployment of resources, alongside a greater reassurance of security for people against crime in general. When combined with artificial intelligence and machine learning to process all of this data at speeds beyond any human scope, very different outcomes may begin to become possible[38]; it could highlight any crime mitigation problems or opportunities human operators may have missed, but on a much larger scale, with a human reviewing each suggestion of course. This sounds ideal, but the balance between more authoritative policing of society and privacy arguments is one which is very delicate, and will ultimately be determined by the people, for the people, at the polls.

With such a controversial topic at stake, undoubtedly many high-level debates and case studies of this debate have taken place and continue to take place worldwide. One of the most famous examples of this has been around an individual who leaked thousands of national security documents to the media to expose unconstitutional violations of privacy by the National Security Agency (NSA) of American citizens – Edward Snowden[39]. Whilst his actions were not the only such ever taken, they are perhaps the most iconic of recent times, though other well-known whistle blowers of this century include Katharine Gun and Daniel Hale too. While Snowden considered himself as a 'whistleblower', for exposing numerous privacy abuses, the U.S. government was not of the same opinion, charging him with violations of the Espionage Act 1917 and revoking his passport. This raises a number of questions, chief among which is the requirement for democratically elected government to be subject to public scrutiny and whether this principle still functions; the harshness of the actions against Snowden would certainly suggest a government attempting to villainise Snowden for his 'crimes' rather than to address the clear illegal practices which he exposed to the people[40]. Following the advent of such strong RSA encryption, amidst changing surveillance policies and increasingly secretive agencies, this has become much more difficult to keep in check – the agencies in question may justify themselves internally, but this should only happen with the democratic consent of the people, following a vote of some sort.

[38] Parliament UK (Christie, Lorna). (2021, April 29). *AI in policing and security*. Retrieved from UK Parliament POST: https://post.parliament.uk/ai-in-policing-and-security/
[39] (NPR) Davies, D. (2019, September 19). *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia*. Retrieved from NPR: https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia
[40] Ibid.

Without this happening and considering the intrusive nature of this type of data collection (somehow bypassing RSA encryption, which end-users would not be expecting due the supposedly strong algorithm in use), these activities may amount to a breach of Article 12 of the UDHR.

Section Four: Conclusion

To conclude, cryptography has enjoyed a long and prosperous history. It has gone from a primarily being tool of the elite and military, used to conceal communications for strategic advantage, to providing a vital foundation for our daily activities. It is clear that from the early days of transposition and substation ciphers to complex polyalphabetic systems such as Vigenère and Lorenz, the developments in cryptography have been driven and accelerated by the constant war between cryptographers and cryptanalysts. Notwithstanding, the current era of public key cryptography is the one which has revolutionised the idea of interpersonal privacy, especially in the digital world.

Considering this, it is important to remain emphatic about how challenges in cryptography persist, especially around key distribution and proprietary implementations of this going into a quantum era. The use of standardised protocols has helped, such as publicly tested, robust key exchange flows and constant iteration of these in the context of ever more powerful computing systems, to protect against possible crusades opposing this mode of privacy. Therefore, as the use and strength of encryption generally continues to grow, it becomes crucial for society to utilise, understand and cooperate with the use of modern encryption as far as possible, to keep it secure for everybody; the benefits it brings cannot be overstated, especially by allowing individuals to exercise their digital rights to business while maintaining confidentiality.

Notwithstanding, this same widespread availability also poses challenges for law enforcement and governments striving to maintain national security and monitor economic well-being. Striking the right balance between privacy and security while maintaining the consent and confidence of the public in doing this is essential to addressing legitimate concerns around public safety while upkeeping human rights. This sector of regulation, though, is likely to go through many changes in the near future as lawmakers and courts become more familiar about how each of their decisions could mould the future world in

ways not currently known. Lastly, however, for an increasingly digitally dynamic era, modern encryption currently stands steadfast as a protector of privacy, safety and the fundamental values of human society.

An annotated bibliography can be found from page 16 onwards.

Bibliography With Annotations

(NPR) Davies, D. (2019, September 19). *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia*. Retrieved from NPR: https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia

This source is a summary of an interview between a prominent radio station in the USA and the whistleblower referenced by name in this project. It is therefore, first-hand evidence of a witness to the suppression of digital rights by the United States government. While it may be sensible to question the truthfulness of certain statements in the source, it is overall a likely genuine article. Hence, I have treated it as accurately reflecting the feelings of Mr Snowden with respect to his actions and beliefs in the field of cybersecurity and digital rights.

Aliyu, A.-A. M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. *International Journal of Computer Applications 135, No. 11*, 46-50.

This source is from a prominent journal in the sector of general computer research. As a peer-reviewed journal, the content and information obtained can be trusted to be truthful and reliable. It was written by two members of a university faculty about a topic which is old in its origin but presents some opportunities for development. I have therefore used this source as a factual basis for my exploration of the traditional Vigenère cipher.

Al-Kadit, I. A. (1992). Origins of Cryptology: The Arab Contributions. *Cryptologia*, 106-112.

Originally published in a specialised peer-reviewed academic journal with specific remit for Cryptographic topics, it can be trusted to be an accurate source for this topic. Written by a Saudi Arabian who graduated from Stanford University with a PhD in Electrical Engineering and significant experience in technology companies, it is likely to be factually accurate, though with a perhaps bias towards the Arab influence in the field. As it is well written with no obvious reason to doubt the facts of the article, I have used it to reference the first steps in classical cryptanalysis.

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports 5 100167*.

This article focusses on the psychological motivations of several different types of people who are regarded as 'hackers' by common law. It is published in a peer-reviewed academic journal with support from ScienceDirect (and by extension Elsevier too) marking it out as high quality. The summaries that it provided of the common methods employed by hackers were information-rich, proving useful for my research.

Claude, S. (n.d.). Communication Theory of Secrecy Systems. *Bell System Technical Journal, 28*(4), 656-715. doi:https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

This article was written by one of the pioneers of modern information theory, Claude Shannon, for an in-house scientific journal at Nokia Bell Labs and published by IEEE, both well respected at the time of publication. I have used it as it is essentially first-hand evidence of the intentions of one of the people who heavily influenced how digital technology progressed over the remainder of the century, who had insight into how the digital age would progress well beyond that of his peers.

Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity, 9*(1), 1-14. doi:https://doi.org/10.1093/cybsec/tyad001

This source was published by OUP in the modern, peer-reviewed Journal of Cybersecurity. As such, and being published as recently as 2023, it provides a very contemporary insight into the quantum applications in cryptography from a pair of academic researchers. Therefore, I deemed their article to be of sufficient reliability, very good insight and recent enough to use as a point of reference here.

Gladwin, L. A. (n.d.). Alan Turing, Enigma, and the Breaking of German Machine Ciphers in World War II. Retrieved from https://www.archives.gov/files/publications/prologue/1997/fall/turing.pdf

Likely to have been commissioned by the Government to commemorate a person who helped shorten WW2 to the Allies' advantage, this source contains a lot of information about Alan Turing and his work. Most useful for me were the steps he took, and the processes followed in the gradual decryption of Enigma. The state nature of the publication also implies that the author would have had access to relevant first-hand knowledge available from objects in the National Archives, which would improve the source's accuracy.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & technology, 35(1)*, 3.

This report was published by a respectable journal in the USA. Considering a great deal of material relevant to the protection of privacy and interpretation of common law in cyberspace, I found it useful to read and consider points from. The breadth of relevant topics covered was also extremely useful, all appropriately referenced using legal precedents and other cases. Thus, the likelihood of its accuracy is high, and the quality of points was very good and appropriate to be used for reference here.

IBM. (2021). *Size considerations for public and private keys*. Retrieved from IBM Documentation: https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys

This source is from IBM, a major company in the IT industry. This source was purely factual and to indicate an idea of key sizes used in cybersecurity in the modern world. IBM's reputation and influence in the industry provide evidence for the assertion that these figures are researched and reliable for use in this research project.

IBM: Dames, Anne; Richuso, Emily. (2022, March 10). *What is Quantum-Safe Cryptography, and Why Do We Need It?* Retrieved from IBM: https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it

This was also written by employees at IBM on behalf of the company and so conforms to the same reputational implications of reliability as the previous source. The article considers some of the consequences associated with the advent of quantum computers, with a specific section on cryptography too. For these reasons, written by professionals at a world-leading company, I considered it a reliable and useful source.

IETF. (2023). *OAuth 2.0 Security Best Current Practice*. Retrieved from IETF Documentation: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics

OAuth 2.0 by the Internet Engineering Task Force (IETF) is one of the principal standards used by companies with secure digital presences to ensure that they follow the best practices for maximum security. Being the standards themselves, this source is very good in explaining the protocols and their purposes in an accurate fashion. The IETF has also been operated by a worldwide non-profit organisation, not under the current influence of a territorial government.

Kessler, G. C. (2015). *An Overview of Cryptography*. Auerbach.

Dr Gary Kessler is an academic consultant and practitioner in the sector of maritime network security and protocols, having retired as a professor of cybersecurity from Embry-Riddle Aeronautical University in the USA. He is an accomplished author of research and explanatory papers on the topic of cybersecurity. With this, he has written this specific source to make the topic more accessible to the unfamiliar. Owing to his academic success in the field, reliability of the source is assumed.

National Cyber Security Centre. (2020, November 11). *Preparing for Quantum-Safe Cryptography*. Retrieved from NCSC GOV UK: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

The National Cyber Security Centre is run by the UK Government, but its remit is generally to help mitigate cyberattacks that have damaging effects on businesses and individuals nationwide. This is a whitepaper (a policy document setting forward future plans) so may be slightly biased towards favouring the sort of regulation currently awaiting passage through Parliament, however, can be considered generally accurate factually.

Office for National Statistics (ONS). (2023, April 27). *Crime in England and Wales Statistical bulletins*. Retrieved from ONS (GOV UK): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/previousReleases

The ONS is the primary public statistical body in the UK. It collects and collates data from a variety of general and public authority sources. For this reason, the statistics it collects, publishes, and analyses are unlikely to show any significant bias or untruthfulness in the current political climate as it operates independently of the Government, reporting instead directly to Parliament.

Onwutalobi. (2011, January). Overview of Cryptography. doi:10.2139/ssrn.2741776

This source was published on SSRN by an author who is most likely to have been a higher education student at the time. Consequently, I have treated this source with caution, however, it does appear to be truthful, not disagreeing with any other source here, and factual in its statements which I have used here.

Parliament UK (Christie, Lorna). (2021, April 29). *AI in policing and security.* Retrieved from UK Parliament POST: https://post.parliament.uk/ai-in-policing-and-security/

This was written and published by the Parliament UK POST division. Its official function is to '[source] reliable and impartial scientific research for Parliament', written by sufficiently qualified academic staff. It is designed to be impartial and sufficiently factual such that nationally significant decisions can be made on the basis of its reports; it is also reviewed before publication. Therefore, it is also sufficient for the purposes of this project.

Parliament UK. (1998). *Human Rights Act.* London: National Archives UK.

Parliament UK. (2016). *Investigatory Powers Act.* London: National Archives UK.

These are two laws which are relevant to some of the discussion present in section three. They were voted through Parliament and given Royal Assent to be enacted during their respective terms of Parliament. Published by the National Archives, there is no argument possible about their truthfulness as they are UK common law by definition. It is not unfair to make general assumptions about similar legislation in many other countries as many legislatures generally come to altogether similar conclusions on this topic, each with their own nuance. However, I used these sources with specific reference to how investigations are conducted in the United Kingdom.

Preetha, M., & Nithya, M. (2013, June). A Study and Performance Analysis of RSA Algorithm. *IJCSMS, 2*(6), 131-134.

Written by two Indian academics about the function, purpose and mathematics around the RSA algorithm, and published by a minor peer-reviewed academic journal, this was an article designed to be informative yet accessible. Due to being peer-reviewed, I considered it to be sufficiently reliable and a suitable source for that section, discussing relevant factors at an appropriate depth.

Singh, S. (1999). *The Code Book.* Fourth Estate.

The Code Book was one of the starting points for me when conducting initial research for the project, providing a reasonably detailed timeline of various events in cryptography, which I researched further using other sources. Its author, Simon Singh, is a well-known mathematical author in the UK, with a PhD from the University of Cambridge and an active interest in research of this sort. Owing to the book's popularity, influence, and the work that went into researching it, this source was fundamental to me and has been treated as factual.

Solso, R. L., & King, J. F. (1976). Frequency and versatility of letters in the English Language. *Behavior Research Methods & Instrumentation, Vol. 8 (3)*, 283-286.

Cited from a peer-reviewed journal published by ScienceDirect and written by esteemed academics, the accuracy of this source can be fairly assumed to be very high. This article was particularly useful when discussing frequency analysis despite being written for a linguistics journal. The types and results of frequency analysis can vary between different researchers, culminating in slightly different results between different surveys, but this should not be taken as a sign of any gross inaccuracies or false inferences in this case as general trends between them are maintained.

United Nations General Assembly. (1948). *The Universal Declaration of Human Rights (UDHR)*. New York: United Nations General Assembly.

This source is fairly self-explanatory. The UDHR is an international document that enshrines the rights and freedoms of individuals of the human race. Its statements cannot be questioned from a factual standpoint, and I have referenced it as a source for one of my more recurrent points in section three.

Vacca, J. R. (2017). Computer and Information Security Handbook (Third Edition). Morgan Kaufmann.

This book represents an overview of cryptography and a great deal of its history. Written by a respected information technology consultant and published by an Elsevier subsidiary is a sign of the good nature and accuracy of its contents. I have taken from it information about the progression of certain ciphers, especially Enigma, which has proven essential in making the explanations of these ciphers more accessible to a general audience.

Wright, E. V. (1939). *Gadsby*. Wetzel Publishing Co.

This is a work of fiction which I have interpreted to have a deeper agenda in its creation. Being a lipogram that deliberately avoids the letter 'e', it was a useful real-world example that frequency analysis of text is not infallible, as opposed to any specific points from the book.