Jack (STUDENT)

How has encryption evolved and can it survive in the age of quantum computing?

Contents

[How has encryption evolved and can it survive in the age of quantum computing? 2](#_Toc150011013)

[Introduction 2](#_Toc150011014)

[What is Encryption? 2](#_Toc150011015)

[A Brief History of Cryptography (Part 1) 3](#_Toc150011016)

[Quantum mechanics and the quantum computer (Part 2) 6](#_Toc150011017)

[Superposition 6](#_Toc150011018)

[Qubits and Quantum Interference 6](#_Toc150011019)

[Entanglement 6](#_Toc150011020)

[The No-Cloning Theorem 7](#_Toc150011021)

[The origins of quantum computing 7](#_Toc150011022)

[What is a quantum computer and what are its capabilities? 7](#_Toc150011023)

[Why is it so difficult to build a quantum computer? 8](#_Toc150011024)

[What threat does quantum computing pose and how can it be mitigated? (Part 3) 8](#_Toc150011025)

[The threat quantum computing poses 8](#_Toc150011026)

[Defending against quantum attacks 9](#_Toc150011027)

[Conclusion 11](#_Toc150011028)

[Glossary 12](#_Toc150011029)

[References 14](#_Toc150011030)

[Bibliography 16](#_Toc150011031)

# How has encryption evolved and can it survive in the age of quantum computing?

## Introduction

Effective, error tolerant quantum computing could become a reality in the next 10 years. When this happens virtually all of the encryption that we rely on to safeguard our privacy and data will become obsolete overnight. With our increasing dependence on the internet and computers, it is more important than ever that our encryption remains strong. In its current state it may not be sufficient to face the quantum threat.

Through my essay I will: explore the evolution of cryptography; investigate how quantum computers function and how they are superior to modern computers; and finally analyse the threat quantum computers pose to existing cryptographic infrastructure and whether it can be mitigated.

I intend to determine through what methods encryption could be modified to become intractable to quantum computers, or if there are any current methods that quantum computers are unable to effectively break.

### What is Encryption?

The word cryptography literally means “secret writing”, with encryption being the procedure behind it. The government define encryption as: “The process of transforming plaintext into ciphertext using a cryptographic algorithm and key” [1]. Encryption is used to conceal data so that unauthorized people cannot read it. Cryptography simply is the study of encryption, and a cipher is what encryption produces – disguised writing that no one else can read.

As the RSA official guide to cryptography explains, the secrecy of encryption is essential: “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?”. [2] Everyone has things they want kept private. Companies have trade secrets. Governments have military strategies. People have credit card details. As a result encryption is more secure now than it has ever been before, but it is also more important. Could the advantages quantum computers have over conventional computers compromise our current encryption methodologies and leave us vulnerable?

## A Brief History of Cryptography (Part 1)

The earliest written evidence of encryption was from 4000 years ago in ancient Egypt, found in the tomb of nobleman Khnumhotep II. It held a script telling of his deeds in life, but unusual hieroglyphs were used which obscured the original meaning of the text.

The ancient Greek generals of Sparta in the 7th century BC later used a type of transposition cipher called a Scytale. Cloth was wound around rods of a specific diameter. The message was written on it, and then the cloth was unwound, scrambling the message. This is a very early form of transposition cipher using the diameter of the rod acting as a key. “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.” [3] This later evolved into the rail-fence cipher, where messages are written out in rows but then sent in columns. In this case, the number of rows would act as the key to the message.

In time, encryption began to be recognised as something useful to generals and governments. One well known example is the Caesar cipher used by Julius Caesar in around 60 BC. This basic substitution cypher involved moving letters along places in the alphabet. Although sufficient at the time it granted very little security: “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.” [4].

While the Caesar cipher involved simply sliding letters along in the alphabet, the simple substitution cipher was slightly more effective. In this familiar, monoalphabetic form of encryption, each letter in the normal alphabet corresponds to another letter in the cipher alphabet and is swapped in the message. As there are thousands of ways you could order the alphabet, guessing it correctly is very difficult. “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” [5] Eventually however, frequency analysis rendered this method obsolete.

Polyalphabetic ciphers were naturally the next step as they used multiple cipher alphabets. One of the earliest was the Alberti cipher, invented in 1467 by Leon Battista Alberti. However due to their more complex nature they did not increase in popularity until 1553 when Giovan Battista Bellaso invented the Vigenère cipher. The multiple cipher alphabets made the Vigenère cipher so tough to break that it was believed to be unbreakable and called “le chiffrage indéchiffrable” - the “unbreakable cipher”. It functioned like a series of individual substitution ciphers all being applied to different letters of the text. “The Vigenère cipher, being a 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”. [6]

Eventually the Vigenère cipher was broken in 1863 by Friedrich Kasiski. “The weakness of the Vigenère cipher lies in its short key and that it 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.”. [7] The Vigenère cipher is commonly misattributed to Blaise de Vigenère who further improved upon it with the invention of the more secure autokey cipher.

By the time World War 1 broke out almost all monoalphabetic and many polyalphabetic substitution ciphers had become obsolete; they were simply too easy to break. Encryption had evolved to the point that codes needed to be invulnerable to frequency analysis and utilise far too many key permutations to search through by hand. Transposition ciphers were unaffected by frequency analysis and many were more difficult to break than equivalent substitution ciphers. They had evolved since the early days of the Rail Fence cipher but were still relatively easy to do by hand. One example of this, Columnar transposition was a popular cipher used in World War 1. In fact, it was so effective that it continued to be used in World War 2 as a double transposition cipher – simply a columnar transposition cipher applied twice. Of all the ciphers in World War 2 that were done by hand, this was one of the most secure. In both world wars hand ciphers were often used for information that went out of date quickly. Hand ciphers were convenient and didn’t require any equipment, but were easier to break. However, the information would be useless by the time the opponent was eventually able to break the cipher.

The main development in cryptography during the world wars was due to mechanical advancements. As electricity and increasingly advanced technology made it possible to create more complex machines some of which would be used for cryptography. Rotor machines were invented in several places at once throughout 1915-17. These were typewriters that incorporated disks (called rotors) that had wires running through them. These wires changed inputs into the disk into different outputs, encrypting them. Furthermore, when a key was pressed the disk would rotate, changing what each letter was encrypted to each time.

The Enigma machine, was invented in 1918 by Arther Scherbius and used several rotors to make it more difficult to break than past mechanical ciphers. This cipher is well known for being used by the German armed forces during World War Two. However, it was not as secure as they believed. It was initially broken by the Polish at the beginning of World War 2, using electromechanical devices called Bombes. However, Poland was invaded by Germany so the Bombes were sent to Britain. Germany later added 2 more rotors to the machine so that any 3 of the 5 rotors could be used. This meant increasing amounts of bombes were required to break the code.

Hitler and his top officials used an even more complex rotor machine called a Lorenz Cipher. This early form of a stream cipher was far too complex for the Bombes and so Britain’s cryptologists broke it by building Colossus - the world’s first computer. Colossus was designed to search through all the possible keys to the Lorenz cipher to find the correct combination of rotors to break it. The decrypts from both the Lorenz and Enigma ciphers were essential in helping the Allies win World War Two, shortening the war by as much as two years.

While the Polish cracked the Enigma cipher and the British broke the Lorenz, there is one cipher that is theoretically unbreakable. In World War Two the British used the one-time pad, a cipher that cannot be broken by brute force or analysis. Even if you somehow already know what part of the plaintext is, every letter is independent so you cannot crack the rest. In 1945 Claude E Shannon published “A Mathematical Theory of Cryptography”. This proved that the one time pad was truly unbreakable, but that any unbreakable system must have certain principles – “the key must be truly random, as large as the plaintext, never reused in whole or part, and kept secret”. QUOTE

A form of cryptography that can never be broken had now been invented. However, one time pads and similar ciphers cannot solve the key distribution problem - all ciphers that use a single key require both the sender and receiver to possess that key. The key could be transmitted over a secure channel, but if you have a secure channel, why not transmit the message itself over it? Another problem is that for unbreakable encryption, the key has to be at least as long as the message and can never be repeated. Every time you use up all your keys, you have to generate a new one and get it to the other party. This was a major limitation, and made it clear that strength was not the only important factor when creating an encryption.

The American company IBM was one of the first to create and sell computers and created the hash function in 1953. This is a form of one way encryption. Any text input can be mapped to a number, which should be unique for the text. For a hash function to be effective, you should not be able to convert the number back into the text. This is commonly used for storing passwords and in zero knowledge proof. You can prove to your computer that you know the password to it, without the computer ever having to store the password. The computer can simply store the hash number of the password and then hash your input and check if it matches.

IBM continued to be a driving force in computer based cryptography. In the 1970s it formed a crypto-group with other companies due to the requirement for an effective and standardised encryption algorithm. The block cipher they developed was called Lucifer and in 1973 it became the DES (Data Encryption Standard) in America, used by the government to securely transmit data. It was eventually found that DES was providing insufficient security and so it was updated to triple DES in 1974; however this was a cumbersome and inefficient method.

Even with the development of computing there was still no solution to the key distribution problem. However, in the early 1970s GCHQ (Britain’s intelligence, security and cyber agency) developed the very first public key cryptography. Public key cryptography conveniently solved this problem by having 2 keys. An initial, private key is created and then a public key is created using the private key plus several other numbers. The trick is it uses a trapdoor function – easy to calculate, but difficult to reverse. It is easy to figure out the public key from the private key, but almost impossible to discover the private key given the public. The public key can only be used to encrypt messages and the private key can only be used to decrypt messages. Therefore the public key can be shared with anyone. If they send a message to you, they encrypt it using the public key and you can decrypt it with the private key. However, as the public key can only be used for encryption, no one else can decrypt it. In reality, public key encryption is far slower than private key, and so it is impractical to use it to transmit messages. It is usually used to transmit private key encryption keys securely, so that faster private key encryption can then be used.

In 1976 Whitfield Diffie and Martin Hellman published the concept of key exchange and public and private key encryption. However, the first widely known form of public key encryption was developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. They created RSA public key encryption, which involved multiplying two massive prime numbers together to get the public key. To crack the encryption you would have to discover the primes given only the public key. This is not a trivial task; “it would take roughly a billion times the lifetime of the universe to check all of them [the keys] and decipher the message” [5].

Elliptic curve cryptography, first suggested by Neal Koblitz and Victor S. Miller in 1985, is another form of public key encryption. It is able to have a shorter key length than other comparable encryption methods, but theoretically provides the same level of security depending on the elliptic curve used. This is still used today, especially for digital signatures in cryptocurrencies such as bitcoin.

**B**y 1997, even the security provided by triple DES was beginning to become insufficient. The National Institute of Standards and Technology announced that they would be taking submissions for a replacement block cipher for DES – to be known as AES (Advanced Encryption Standard). Many groups, companies, organizations and individuals submitted contributions including the MARS cipher developed by IBM. The chosen cipher was the Rijndael cipher developed by two Belgian cryptographers. A modified version became AES which replaced DES by the year 2000 and is still widely used today.

We have now reached a point where cryptography is virtually impossible to break. Both current public and private key cryptography are invulnerable to all but the largest supercomputers. Even if computing power continues to grow, encryption security will easily keep up. However new techniques that defy conventional physics could mean that public key encryption may still become obsolete.

## Quantum mechanics and the quantum computer (Part 2)

“If you think you understand quantum mechanics, you don’t understand quantum mechanics” (Attributed to Richard Feynmann)

Humans generally expect the world to follow the laws of physics. However, at the level of quanta (the tiny particles that make up everything) these rules can be bent. Different phenomena, which may seem alien to those who have studied conventional physics, dictate the properties of the quanta. There are three phenomena in quantum mechanics that are particularly relevant to quantum computing : superposition, quantum interference and entanglement.

### Superposition

The principle of superposition: a quantum particle that can be in a number of states at random is in all possible states, until it is measured and one state is found. For example, a particle may be in any one of several positions. However, until it is measured and found at one of the positions, the particle is considered to be in all of those positions at once. It can be modelled as a wave which covers all of the possible positions. Once it is measured, the wave collapses to a specific point based on probability, which is where the particle is located. The best known example of superposition is Schrödinger’s Cat.

### Qubits and Quantum Interference

Switches are used by conventional computers to store information with either a state of 1 or 0 – but not both. In conventional computers these are known as bits while their quantum counterpart is the qubit. A qubit can be in a superposition of two quantum states, both 1 and 0. This allows the storage of multiple values simultaneously. However, once measured the qubit’s state collapses into one of the possible values based on probability. Quantum interference influences the qubits probability so that the correct output is more likely and the incorrect output is less likely.

### Entanglement

Entanglement relies on grouping particles together - “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” [8].

The idea that two distant objects could have an affect on each other may not be unbelievable. Many things such as gravity and electromagnetic force act over a distance. Magnets, for example do not have to be touching to interact. Forces like magnetism transmit force by transferring tiny particles between the affected objects. However, the speed of these particles is constrained by relativity – they can never be faster than light. In contrast, entanglement acts instantly – there is no time delay between the change occurring at one particle and at another. This would give it an infinite speed.

Entanglement suggests that information could be sent instantaneously without a medium. This would mean ciphers are no longer required as there would be no way to intercept any communications. However, this is not possible. Measurement has an odd effect on quantum particles. When particles that are superposed are measured, they collapse into one state. When particles that are entangled are measured, they lose their entanglement, among other effects. However, to send information, we would have to put our entangled particle into a set state - but this counts as a measurement, disrupting the entanglement.

### The No-Cloning Theorem

This effect of measuring on quantum particles does not only apply to entanglement. It also led to the no-cloning theorem. The no-cloning principle states that no quantum particle can be fully copied. To copy a quantum particle, you first have to measure everything about the original particle to replicate it. However, measuring the original particle causes it to change. You can produce a new particle that is identical to the old one, but the old one has been changed by the measuring. This effect is of great value in Quantum Key Exchange.

### The origins of quantum computing

“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.” [9] Feynman’s theoretical computer appeared to be of largely scientific value and so was overlooked by governments. However, in 1994 Peter Shor developed a quantum algorithm that could be used to break encryption. Being able to run this algorithm (requiring a quantum computer) would give the possessor a substantial advantage which led to interest in developing such a machine. The first US-government sponsored conference on quantum computing occurred in the same year. In 1996 Lov Grover developed another algorithm, this time to increase the speed of database searches (which also has applications in encryption).

It was not until 1998 that the first quantum computer was finally developed at MIT. However, the computer only had 2 qubits (a carbon atom and a hydrogen atom). It was only in 2001 that Shor’s algorithm was finally put into use. In 2011, a company called D-Wave Systems developed a quantum annealing computer (the most basic form of quantum computer) called D-Wave One, which claimed to be the first commercially available quantum computer. Google alleged to have reached quantum supremacy in 2019, performing operations in 200 seconds that would take a supercomputer about 10,000 years. However, techniques used to optimise supercomputers mean that it would have taken 2.5 days, invalidating the claim. Finally in 2020 a group at the University of Science and Technology of China led by Jian-Wei Pan reached quantum supremacy. To model the particles that took their quantum computer 200 seconds, a classical supercomputer would require 2.5 billion years of computation.

### What is a quantum computer and what are its capabilities?

A quantum computer is a computer that uses quantum phenomena to store data and carry out computations. The computers make use of tiny particles that can utilise the properties of quantum mechanics to do incredible things at extraordinary speeds. “…a quantum computer could do anything a normal computer could do, and, crucially… 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.” [8]. However, it is not as simple as just being a quicker computer. “Each operation may not be faster, however the number of operations necessary to arrive at a result using particular algorithms is exponentially small.“ [10].

Not all types of quantum computer have the same capabilities. Quantum annealers are the simplest type of quantum computer to make and effective ones already exist. They are almost always as slow as or worse than conventional computers, except with optimization problems. Analogue quantum computers are harder to build, but more effective. They can simulate quantum effects and interactions that a normal computer cannot, in addition to being able to solve optimisation problems. A true universal quantum computer is the holy grail. Analog quantum computers and annealers are difficult to use and require teams of scientists to run. A universal quantum computer would be a combination of conventional computer and quantum computer. There is no restriction on what it can be used for – it fulfils all the purposes of a conventional computer, analogue quantum computer and annealer. “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.” [11].

### Why is it so difficult to build a quantum computer?

#### Decoherence

Each qubit in the quantum computer is generally composed of some kind of particle that is entangled and/or superposed. However, quantum particles leak quantum information into the environment, causing superpositions and entanglements to collapse over time, leading to errors – this is called decoherence. Decoherence times in quantum computing can be as short as 2 milliseconds, and since all calculations have to be carried out before the qubits decohere, quantum computing requires longer coherence times before it can be effective.

#### Error correction

Even if quantum decoherence times improve in general, some individual qubits will still decohere or have errors. Therefore, you need an error correction scheme. The simplest might be to store all data twice. This would however mean that twice as many qubits would be needed, a daunting prospect considering the difficulty of creating and using them. While there are no doubt more compact correction schemes, extra qubits are still always required. “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.” [11]

## What threat does quantum computing pose and how can it be mitigated? (Part 3)

### The threat quantum computing poses

Quantum computers have parallel processing capabilities that give them a substantial advantage over conventional computers in certain fields. However, algorithms have to be specifically tailored to make use of these abilities, and without them a quantum computer is no better than a classical one. There are two key algorithms that allow quantum computing to make use of their advantages to break our encryption.

#### Shor’s algorithm

One of the most pivotal moments in quantum computing was the development of an integer factorization algorithm in 1994 by Peter Shor. Public key cryptography (which we use every day) relies on trapdoor functions, as we have already discussed. However, Shor’s algorithm can reverse the two most common trapdoor functions incredibly quickly, rendering many forms of public key encryption ineffective. “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.” [12]. The exponential speedup this algorithm offers is sufficient to make cracking encryption doable within a reasonable time frame. The algorithm works by turning the factoring problem into the problem of finding the period of a function – this part works on classical computers. The second part finds the period of the function using the quantum Fourier transform (this is the part that requires a quantum computer and gives the speedup).

#### Grover’s algorithm

The second algorithm for codebreaking, invented by Lov Grover in 1996 was simply intended to speed up searching though lists. If searching through 1 item in an unsorted list takes 1 second, searching through n items in a list usually takes n seconds. Grover’s algorithm however is able to search n items in the list in the square root of n seconds. This algorithm was supposed to make searching large, unordered databases faster. However, brute forcing an encryption works by searching through a list of possible keys. Thus, this algorithm makes attacks on private key encryption faster. A 256 bit key could be broken in 2128 operations instead of 2256. This cuts the security of the algorithm in half.

### Defending against quantum attacks

Creating quantum secure encryption may be considered a problem for the future. No quantum computers can currently break codes because we can’t make a computer with enough qubits. The closest a quantum computer has come to breaking a code is factoring 15 into 3 and 5. 15 is a 4 bit number, but most encryption keys are 128 or more bits. However, an adversary could store your encrypted messages until a quantum computer becomes available. Then they would be able to break them with ease. Therefore, if people need data from the past to remain secure, they must utilise quantum-intractable encryption before quantum computing becomes available. Often, in cryptography messages have a time limit, a sell-by-date after which it no longer matters if they are secure. You may only need your data to be secure for 5 years. But to achieve those 5 years of security you have to have a way to protect your messages 5 years before quantum computers start breaking codes. However, while current encryptions are vulnerable to quantum-based attacks there are methods we can use to mitigate the threat that they pose.

It is much easier to defend against Grover’s algorithm than Shor’s. Grover’s algorithm reduces the computing to break 256 bit keys from 2256 operations to merely 2128. , While a 256 bit key is virtually uncrackable with classical computers this algorithm would reduce its security to that of a 128 bit key – only half as secure. However, if you double the key size a 512 bit key will still require 2256 operations – virtually uncrackable. While this may result in slightly slower speeds to encrypt, with modern technology it will mostly be unnoticeable. It has been proven that a exponential speed up (like that for breaking public key cryptography) for database searching algorithms is impossible. This means that private key encryption can remain secure in the era of quantum computers.

Shor’s algorithm poses a much greater threat to encryption than Grover’s. Shor’s algorithm is able to reduce the timeframe required to break public key encryption with a super-polynomial speedup. Merely increasing the key size would be totally insufficient to solve the problem. Therefore, there are 2 logical ways to defend against this sort of attack. Develop an encryption algorithm that does not use a trapdoor function affected by Shor’s algorithm; or develop an algorithm for which the super-polynomial speedup is insufficient (the function would still take an absurdly long time to reverse even after the speedup). There are many algorithms being developed that fulfil these requirements. However, most are in some way worse than conventional algorithms. They are slower to encrypt, or require larger key sizes to provide the same security. Because of this, “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.” [13]. A new trapdoor function would be required to create this new algorithm. One popular example is lattice-based cryptography. “Unlike RSA, rather than multiplying primes, lattice-based encryption schemes involve multiplying matrices. The shortest vector problem (SVP) is an NPhard problem […] 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.” [14]. A quantum computer would be no more effective than a classical computer at breaking lattice-based encryption, so this could be used to replace existing, vulnerable algorithms. Another example is multivariate cryptography, based on solving equations with multiple variables, which are hard to solve using brute force. However, transitioning to these new quantum-resistant algorithms will require the redesign of large amounts of software to make use of them. This may take some time, especially as the process should begin before a quantum computer that can break encryption is developed. This makes it all the more important that software is designed to be crypto-agile – designed to be modular regarding what encryption it uses.

Quantum Key Distribution (QKD) is another method of defending against Shor’s algorithm (and any other method of breaking public key encryption). QKD is a system making use of quantum properties to allow us to exchange private key encryption keys over an unsecured channel. This does not make public key encryption secure against quantum attacks, but would rather replace public key encryption for securely transferring/establishing private key encryption key. It uses the no-cloning theorem and the effects of measurement on quantum particles to detect eavesdropping and interception. “The message transfer begins by one party sending a stream of photons to another; the state and characteristics of each photon 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. Because silent interception is not possible, and the key is completely random, the quantum key is virtually unbreakable” [15]. It will remain secure no matter how powerful computers become, as it depends on quantum phenomena for its security, rather than the time taken by current computers to solve a mathematical problem. “A fully quantum cryptosystem can resist attacks generated from a quantum computer, which employs quantum channels and qubit as the medium of communication and computational units, respectively.” [16] However, while QKD is powerful, like the one time pad it cannot simply be used to solve every problem. QKD requires specialised and expensive hardware to carry out, and a physical connection between the two parties. It has only been carried out over limited distances and this would cause problems if we attempted to implemented for security over the internet. The cost and difficulty of creating the infrastructure would make it virtually impossible on a large scale. It could be still used for security at key sites e.g. government installations.

## Conclusion

Encryption has evolved over thousands of years, gradually improving to face new threats and methods of attack. It has reached the point where it has become invulnerable to current computers and is the most secure it has ever been. However, even as encryption has become tougher to break, quantum computers have started to develop from concepts into machines capable of massive parallel computation. When they reach their peak, they will be able to break many of the ciphers we use today with ease. The most common public key encryption schemes are highly vulnerable to attack by these advanced machines.

However, I still believe that encryption will survive in the age of quantum computing. While current public key encryption schemes using certain mathematical functions (for example RSA with the integer factorization problem) will not survive, there are methods of defending against quantum computing that mean that encryption as a whole will remain. Private key encryption would be largely unaffected (although key sizes would have to increase). New public key encryption schemes using lattice-based problems or other quantum intractable functions could be developed, or we could use quantum key distribution to prevent eavesdropping while exchanging keys. Encryption will have to adapt to the new attacks it will become vulnerable to but once action is taken to replace the weakened systems it will be as strong as ever.

## Glossary

|  |  |
| --- | --- |
| Term | Definition |
| Block Cipher | This is a form of cipher where the encryption algorithm operates on fixed-length sections of the message (blocks). |
| Brute force decryption | A brute force attack relies on systematically trying every possible key to an encryption until the correct one is found. |
| Ciphertext | This is the resulting message after encryption is applied to the initial message. |
| Code | A code is a form of encryption where each word in the message is replaced with a letter or symbol using a dictionary of code-to-letter mappings (called a codebook). |
| Frequency Analysis | A method of breaking substitution ciphers by looking at the frequency of letters, pairs of letters or words in the ciphertext. |
| Key | A cryptographic key is a piece of information, usually a string of numbers or letters which when processed using an algorithm, can be used to encrypt or decrypt messages. |
| Monoalphabetic cipher | A monoalphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced with a corresponding letter in a single reordered alphabet. |
| Plaintext | The text or message before it is encrypted. |
| Polyalphabetic cipher | A polyalphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced with a corresponding letter from one of multiple reordered alphabets. Which alphabet is used is determined by a specific rule. |
| Quantum Fourier Transform | The Quantum Fourier Transform is a function that transforms delta functions into sinusoidal wave functions. This reveals the phases or patterns in a superposition. |
| Schrodinger’s cat | In this thought experiment there are four elements: a cat, an airtight box, a vial of poison and a radioactive source. Radioactive sources decay at random based on probability. The cat is put in the box with the radioactive source and the poison. When the radioactive source decays the poison will be released and the cat will die. However because we cannot see inside the box the cat could be alive or dead. Therefore until the box is opened the cat is both alive and dead. This experiment was originally intended to mock the concept of superposition as the cat is either alive or dead at the end of the experiment. However this does still conform to the rules of quantum mechanics as opening the box and seeing the cat is the point at which the wave collapses and the outcome becomes definite. |
| Stream Cipher | This is a form of cipher where the algorithm and key are applied to the message one binary digit at a time. |
| Substitution Cipher | A substitution cipher is a cipher which changes what letter is in each position based on the original letter, an algorithm and usually a key. |
| Transposition Cipher | A transposition cipher (also known as a permutation cipher) is a cipher which scrambles the positions of the letters without changing what the letter is. |
| Zero-knowledge Proof | A zero-knowledge proof is a method by which one party can prove to another party that a statement is true, while avoiding conveying any information about the statement other than that it is true. |

## References

[1] Computer Security Resource Center, “encryption” 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, May 2019

[2] S. Burnett, S. Paine, “RSA Security’s Official Guide to Cryptography”, USA, RSA Press, 2001

[3] Tresorit, “The history of encryption: the roots of modern-day cyber-security”, https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/, 14 Jan 2022 [Online]

[4] RedHat (H. Sidhpurwala), “A Brief History of Cryptography”, https://www.redhat.com/en/blog/brief-history-cryptography, 12 Jan 2023 [Online]

[5] S. Singh, “The Cracking Codebook”, UK, HarperCollins Publishers, 2001

[6] K. Rabah, “Theory and Implementation of Data Encryption Standard: A Review”, Information Technology Journal, April 2005 [Online], available at 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

[7] A. Lia Hananto, A. Solehudin, A. Susilo Yuda Irawan and B. Priyatna, “Analyzing the Kasiski Method Against Vigenere Cipher”, https://arxiv.org/abs/1912.04519, 10 Dec 2019 [Online]

[8] B. Clegg, “The God Effect”, USA, St Martin’s Press 2006

[9] E. Rieffel, W. Polak, “An Introduction to Quantum Computing for Non-Physicists“ https://dl.acm.org/doi/pdf/10.1145/367701.367709, 3 Sept 2000 [Online]

[10] C. Mathas, “The Basics of Quantum Computing”, https://www.edn.com/the-basics-of-quantum-computing-a-tutorial/, 13 Aug 2019 [Online]

[11] M. Swayne, “What Are The Remaining Challenges Of Quantum Computing?”, https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/, 24 Mar 2023 [Online]

[12] J. Aumasson, “The impact of quantum computing on cryptography”, https://www.sciencedirect.com/science/article/abs/pii/S1361372317300519, Jun 2017 [Online]

[13] W. Barker, William Polk, Murugiah Souppa, “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms”, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf, 28 April 2021 [Online]

[14] T. Niraula, Aditi Pokharel, Ashmita Phuyal, Pratistha Palikhel, Manish Pokharel, “Quantum Computers’ threat on Current Cryptographic Measures and Possible Solutions”, https://www.mecs-press.org/ijwmt/ijwmt-v12-n5/IJWMT-V12-N5-2.pdf, 2022 [Online]

[15] Z. Kirsch, “Quantum Computing: The Risk to Existing Encryption Methods”, https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf, 15 Dec 2015 [Online]

[16] P. Bikram, “Design and Implementation of Lattice and Chaos based Post-Quantum Cryptography Algorithms”, http://gyan.iitg.ac.in/handle/123456789/2258, 2023 [Online]

## Bibliography

Ajit Narayanan, “Quantum computing for beginners”, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c5a58aa3662b027a1d5ae38f460ddc0edf16e2d0, 1999 [Online]

Alex Biryukov, Christophe De Canniere, “Data Encryption Standard”, https://orbilu.uni.lu/bitstream/10993/17076/1/Data-Encryption-Standart-DES-Encyclopedia-article.pdf, 2011 [Online]

Anne Broadbent, S´ebastien Lord, “Unclonable Quantum Encryption Via Oracles“, https://arxiv.org/pdf/1903.00130.pdf, 8 Oct 2019 [Online]

Axel, “Encryption: The Past, Present And Future”, https://www.axel.org/2021/05/28/history-of-encryption/, 28 May 2021 [Online]

Charles H. Bennett, Ethan Bernstein, Gilles Brassard, Umesh Vazirani, “Strengths and Weaknesses of Quantum Computing“, https://arxiv.org/pdf/quant-ph/9701001.pdf, 12 Dec 1996 [Online]

Dan Froomkin and Amy Branson, “Deciphering Encryption”, https://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm, 8 May 1998 [Online]

Daniel J. Bernstein, Tanja Lange, “Post-quantum cryptography – dealing with the fallout of physics success“, https://eprint.iacr.org/2017/314.pdf, 2017 [Online]

Dirk Rijmenants, “Is One-time Pad History?”, https://www.ciphermachinesandcryptology.com/papers/is\_one\_time\_pad\_history.pdf, May 2022 [Online]

Donald Krambeck, “Fundamentals of Quantum Computing”, https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing, 6 Aug 2015 [Online]

Douglas Selent, “Advanced Encryption Standard”, https://www2.rivier.edu/journal/roaj-fall-2010/j455-selent-aes.pdf, Fall 2010 [Online]

Douglas Stebila, Michele Mosca, “Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project”, https://link.springer.com/chapter/10.1007/978-3-319-69453-5\_2, 20 Oct 2017 [Online]

Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, Tanvi Madhekar, B.S. Thakare, “Brief History of Encryption, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b861e8de6f3fa5e7aba25d06daa5fa7d45f54f93, Dec 2015 [Online]

Evgeny Milanov, “The RSA Algorithm”, https://pdfdirectory.com/pdf/0702-the-rsa-algorithm.pdf, 3 Jun 2009 [Online]

Fauzan2001, “A Brief History of Cryptography“, https://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html, 20 May 2008 [Online]

George Johnson, “A Shortcut Through Time – The Path To The Quantum Computer”, 2003

GIAC (Roger A. Prichard), “Global Information Assurance Certification Paper”, “History of Encryption”, https://www.giac.org/paper/gsec/1555/history-encryption/102877, 26 Jan 2002 [Online]

Jeff Desjardins, “The 3 Types of Quantum Computers and Their Applications”, https://www.visualcapitalist.com/three-types-quantum-computers/, 14 Mar 2016 [Online]

John Gribbin, “Computing with Quantum Cats”, 2013

Kuriakkottu Amalraj Rajan, “Use of Transposition Cipher and its Types”, https://journal.ijresm.com/index.php/ijresm/article/view/1556, 2 Dec 2021 [Online]

Marco A. Barreno, “The Future of Cryptography Under Quantum Computers”, https://digitalcommons.dartmouth.edu/cgi/viewcontent.cgi?article=1022&context=senior\_theses, 21 Jul 2002 [Online]

Milica Djekic, “A Scytale – Cryptography of the Ancient Sparta”, http://ozscience.com/technology/a-scytale-cryptography-of-the-ancient-sparta/, 2013 [Online]

R.A. Mollin, “Cryptgraphy – A Brief History”, https://cubo.ufro.cl/ojs/index.php/cubo/article/view/1645/1496, March 2004 [Online]

Roger A. Grimes, “Cryptography Apocalypse – Preparing For The Day When Quantum Computing Breaks Today’s Crypto”, 2020

S.M. Naser, “CRYPTOGRAPHY: FROM THE ANCIENT HISTORY TO NOW, IT'S APPLICATIONS AND A NEW COMPLETE NUMERICAL MODEL”, https://www.researchgate.net/publication/353999208\_CRYPTOGRAPHY\_FROM\_THE\_ANCIENT\_HISTORY\_TO\_NOW\_IT'S\_APPLICATIONS\_AND\_A\_NEW\_COMPLETE\_NUMERICAL\_MODEL, July 2021 [Online]

Susan Landau, “Standing the Test of Time: The Data Encryption Standard”, https://www.ams.org/journals/notices/200003/fea-landau.pdf?trk=200003fea-landau&cat=collection, Mar 2000 [Online]

Thales Group, “A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY)”, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption, 1 Feb 2023 [Online]

Tony M. Damico, “A Brief History Of Cryptography”, http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography, 2009 [Online]

Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Duˇsek, Norbert L¨utkenhaus, Momtchil Peev, “The Security of Practical Quantum Key Distribution”, https://arxiv.org/pdf/0802.4155.pdf, 30 Sept 2009 [Online]

Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography“, https://arxiv.org/pdf/1804.00200.pdf, 2018 [Online]

Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, “Elliptic Curve Cryptography”, https://dl.acm.org/doi/pdf/10.1145/1386853.1378356, May 2008 [Online]

William Buchanan, Alan Woodward, “Will quantum computers be the end of public key encryption?”, https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1226650, 20 Sep 2016 [Online]

Yoshito Kanamori, Seong-Moo Yoo, “Quantum Computing: Principles and Applications”, https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1410&context=jitim, 2020 [Online]

Yumnam Kirani, “Generalization of Vigenere Cipher”, https://www.researchgate.net/profile/Yumnam-Kirani/publication/235741546\_Generalization\_of\_Vigenere\_cipher/links/0fcfd51304111ad522000000/Generalization-of-Vigenere-cipher.pdf, Jan 2012 [Online]