How Future-proof are Current Standards of Encryption?

With a focus on Quantum Computers

Alasdair Koplick – XFF6176

City of London School

04/05/18

Table of Contents:

How Future-proof are Current Standards of Encryption?

Encryption, whether allowing governments to securely send secret and confidential documents or making sure you can talk with your friend without anyone else eavesdropping, underpins our modern world. Our ability to send data between computers securely, without compromising on speed is essential to almost any operation made by you, me, corporations, the government, or just about anybody. However, Public Key technology, the basis on which our current standards of encryption stands, has been around and used since 1973 (1) (Arthur, 2013) (having been developed by GCHQ), as reported by Charles Arthur, technology editor for the Guardian. Although encryption has been upgraded, as computers have grown more and more powerful, we currently stand on the verge of a Quantum Computing revolution, with specific-use Quantum Computers already in existence and the first general use Quantum Computers soon to follow. These machines will harness the fundamental properties of Quantum particles and the laws of nature in order to achieve computational speeds that no classical computer would ever hope to match. Our current systems of encryption have never seen a greater threat, but does our encryption have the strength to even be considered as a suitable form of encryption in the face of this new, Quantum threat? In this dissertation, I will be looking at how secure today's current encryption will be in the future against Quantum Computers and other such threats, and as it looks increasingly like our standards of encryption will eventually be breached by Quantum Computers, I will also be discussing our main defence against the Quantum onslaught. I will not just be assessing whether we need to overhaul and revamp our standards and procedures for encryption (or if it is even worth keeping our current system), but also how a move to an entirely different system of encryption may be the only thing to save us. I came to this topic for my dissertation through chapter 9 of the online course looking at an introduction to cryptography, and further decided to develop it by looking more at encryption (which is a running theme throughout all of the online material, as it is a very important area in Cyber Security), and my own interest in Quantum Computers. My dissertation will first focus on what Quantum Computers are (Emerging Super-Computers), and then will look at encryption in detail (History of Encryption) before considering how the two will face off (Quantum Computers Vs Encryption), before looking at our best defence against Quantum (The Solution) and finally moving onto other threats that encryption may have to face in the future outside of Quantum Computers (Other Threats Facing Encryption), and my conclusion.

Before I get any further in this dissertation, it is necessary to define some key terms.

- Encryption is "the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot" (2) (Encryption, 2018).
- Qubits, or Quantum bits, are the bits that Quantum Computers operate in and are different to classical bits in that they can have a value of 0 or 1 or a third value of both 1 and 0 (in a Quantum superposition).
- "Keys" are strings of numbers which can be used to encode and decode messages by computers, keys come in different numbers of bits; for example a 64bit key has 2^{64} digits in the string of numbers that make it up.
- Key Distribution is the system by which we distribute keys between server and connected computers, this should be as secure as possible, as anyone eavesdropping might learn how to decode the encoded messages sent between the server and receiver.
- A cryptosystem is the whole system of generating keys, distributing the keys, encoding, decoding.

I will also be talking about two different types of computer, described here:

- Quantum Computers: that make use of "Quantum-mechanical phenomena" in their operation (defined further in first section, see below).
- Classical computers: normal computers that you or I are familiar with, which use classical bits in their circuits instead of Qubits.

Emerging Super-computers: Qubits, Quantum Power and Faster Computers

Before we can look at the threat Quantum Computers pose to encryption, and the reason so many Cyber Security specialists are worried about the future, we need to understand more about how Quantum Computers work, and the differences between Quantum and classical computers. Let's start with a definition from a Wikipedia article updated last month: Quantum Computers are computers "that use Quantum-mechanical phenomena" (3) (Quantum Computing, 2018) to achieve much more faster and/or complex operations that classical computers, as they utilize Quantum particles instead of electrons in their circuitry. As a result, they deal in Qubits (standing for *Quantum bits,* which can either have values of 0, 1 or a third value that is a superposition of 0 or a 1). When looking at Quantum and classical in the computing world, this is one of the most important differences; the two types of machine are fundamentally different down to the very electrons that flow inside the circuits, and the use of Qubits instead of classical bits inside these machines, gives it a lot more processing power (for certain operation,

see section on). However, despite the immense power inside these machines because of its Quantum properties, the Quantum properties themselves mean that any Quantum Computing Device has drawbacks. Firstly, the machine (or the circuitry) must be kept very cold to prevent Quantum decoherence, where the electrons inside the circuitry would lose their Quantum properties - rendering the machine useless. Secondly, and more importantly in the case of encryption, Quantum Computers, because of their very nature, can only be used for solving specific tasks (although general purpose Quantum Computers are likely to follow shortly after the advent of the first commercial specific use Quantum Computers). On top of this, because the temperatures that need to be reached to prevent decoherence are so low, the computer can only solve problems for a short period of time (a few seconds). Yet despite these drawbacks, the power of these machines has enabled them to solve unsolved problems (within the short space of time available to them) in ways that classical computers could not solve them. This is why people are worried about encryption. It's very hard for classical computers to factorise large numbers, the task requires a lot of processing power (some of the strongest encryption could take classical computers millions of years), and encryption relies heavily on this fact. The public and private "keys" are actually just very, very large numbers. But Quantum Computers can solve issues in ways that classical computers simply can't, because of their Quantum properties, and research suggests that encryption that might take decades or centuries for a classical computer to solve, could be solved in mere seconds or minutes by a Quantum computer. Despite the limitations imposed on Quantum Computers by their design and the particles they make use of, their power is still immense. Theoretically, Quantum Computing Devices will be able to reduce the time taken by classical computers for some intensive operations from millions of years, to days, hours or minutes. This is why encryption experts are worried; solving encryption quickly and easily is within the reach of Quantum.

History of encryption: Romans, One way functions and Public Keys

Before we can understand the threat that Quantum Computers pose to our systems of encryption and secure communication on the Internet, we need understand what the fundamental concepts and ideas behind encryption are (from the most basic cipher, to the our own online key distribution systems), and how we use it for secure communications on the Internet. Despite only coming into use in everyday language since the advent of the Internet, encryption has been around for quite a while. Around 2200 years ago in 200 AD, Roman generals on campaign would encrypt messages before sending them up the chain of command; in the case that the messengers carrying them were ever caught and killed, the message would not be able

to be read and the enemies would not have gained any information. The Romans used a relatively simple encryption method called the Caesar Cipher (inset above (4) (Caesar Cipher, 2018)), which essentially worked by offsetting every letter by a certain amount, so for example: "Greetings from Claudius" would become "juhhwlqjv iurp fodxglxv" when shifted by 3 letters (4) (Caesar Cipher, 2018).

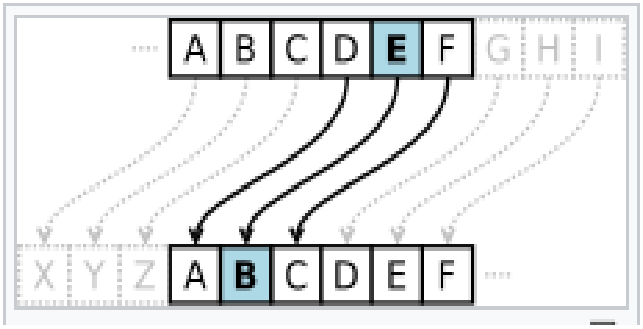


Diagram showing the Caesar Cipher.

Although this is incredibly simple in retrospect, many enemies were very confused by these encoded messages, and the failsafe of encryption certainly helped the Romans with their military victory. That idea; that any third party who unintendedly receives or intercepts the message will not be able read it, is the essence of encryption, and is still alive today on the Internet, although in a very different form. Modern day encryption really took off at the start of the Cold War (early 1960s), which was also the birthplace of many new computer systems. After seeing the success of Turing's Bombe at cracking the "uncrackable" German enigma code in World War 2, the US took up the reigns of Computer Science, with most of the experts moving over to the US and large scale collaboration between the US and UK ensuing, including sharing of schematics of the Bombes and other new machines (5) (Corera, 2015), as written by Gordon Corera, the BBC's security correspondent who specialises in computer technology, in his book "Intercept". At this time, most universities or research institutes had a few of these new machines sitting in a basement somewhere (perhaps more if you were lucky) for everyone at the facility to use. Computing time was valuable, so to make sure that no one accidently (or on purpose, perhaps for a joke) messed with someone else's work, MIT deployed (in 1961) the first username and password login system for their CTSS (compatible time sharing system) (6) (History of Encryption, 2012). Although, 5 years after its implementation, a software bug meant that anyone who logged on would see the master list of all the usernames and passwords. Then, in 1979 as computer networks between universities and other facilities across countries started to become more and more connected, and the first public dial-in networks emerged (7) (History of the Internet, 2018), the National Bureau of Standards introduced DES, using a brand new technology:

56 bit encryption. 56 bit encryption means that the secret "key" that was used to encode and decode messages was 2^{56} digits long. Despite this being a huge number, the corresponding Wikipedia (updated last month) page states that 56 bit encryption "represents a relatively low level of security (in the context of a brute force attack)" (8) (56-bit Encryption, 2017). This was pointed out 20 years after DES's introduction after the Electronic Freedom Foundation broke a DES key in 56 hours, and later reduced it to just 22 (6) (History of Encryption, 2012). In response to this, AES (128 and 256 bit) was developed (1997) and first published in 1998. However, there remained a serious issue; both AES and DES were "Private Key "cryptosystems. Indeed every cryptosystem up until this point had been a "Private Key" system. This meant that you kept your "key", which you used to encode your message to yourself. This makes sense, if you gave your "key" away and it fell into the hands of someone you didn't want to read your message (using the Caesar Cipher as an example, if you accidentally told an enemy spy how places to shift each letter), then your message would be compromised. But on the Internet, how is the server supposed to send the computer connected to it the key to encrypt? If the server sends it over the network, then any eavesdropper would also have the key, and be able to decrypt any messages sent from the server to the computer, or vice versa, making the encryption pointless. The answer, is Public Key encryption, and when it was proposed, it flew in the face of 200 years of established cryptography.

Public Key encryption is the single idea underlying (almost) all modern encryption on the Internet, and as a result, is extremely important for understanding both the strength of today's cryptosystems, and encryption on the Internet in the future. In Public Key encryption, the server generates a very large number (often 256 bit or greater). This number is then used to generate two keys (instead of one). One key is called the Public Key, and can only encode messages, the other key is called the Private Key, and can only decode messages. The server keeps the Private Key to itself, but hands out the Public Key to any computer on the network that asks for it. This means that the computers communicating with the server can send encrypted messages to the serve, that only the server can read. However, the server can't yet send encrypted messages to the computers. What happens now is that the computer uses the servers Public Key, to encrypt its own set Public Key that it already created (whilst keeping its corresponding Private Key to itself), and sends it to the server. Now both the server and the computer can communicate securely with each other, without an eavesdropper knowing anything more than how to encrypt messages to send to the server. This was such a brilliant and revolutionary idea at the time, that when it was originally proposed,

However, despite solving the biggest issue when it came to Internet security and eavesdropping, Public Key encryption functioned not too far out from Private Key encryption. Both relied on generating keys, and (more importantly for looking at Quantum Computers and the future of our encryption) both relied on one way functions. One way functions (illustrated below (Foundations of Coding: Compression, Encryption, Error Correction, 2015)(20)) are the second most important idea in Internet encryption, and are the reason that the US government is offering money for people who can find the largest prime numbers, and why it's illegal to have certain other prime numbers (written down) in your possession.

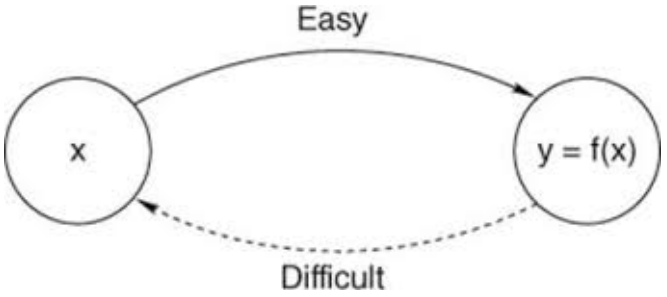


Diagram demonstrating a one way function.

One way functions are mathematical operations that are very easy to do one way, but nearly impossible to do the other way. For example, in Private Key encryption, if you have your key, then it's very easy to encrypt a message, but you also want it to be as hard as possible to decrypt the message (unless the other person also has the key), whereas in Public Key encryption, you want to easily be able to generate a Public Key (for encoding) from a Private Key, since you need to redistribute them every few seconds, but you want it to be almost impossible to make a Private Key (for decoding) from a Public Key, especially since you are giving the Public Key out to anyone who joins the network. And secure encryption relies on this one way function being, well, one way. To ensure this, the keys that are used are huge numbers (often larger than 2^{256}, as I mentioned earlier), and as a result, if a new key is distributed only every 10 seconds, the probability of a brute force attack guessing the correct key is astronomically low. Yet Quantum Computers might be able to get around this hugely unfavourable probability; and to do so would break all of the security that the Internet has been built on.

Quantum Computers Vs Encryption: Will it Break or Will it Hold?

In 1995, mathematician Peter Shor, a leading expert on the two fields of Quantum Mechanics and Computer Science that at the time were coming ever closer together, published a paper called "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" (9) (Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, 1995), the contents of the paper described a fascinating

sort of algorithm, later named Shor's algorithm. This paper and algorithm was of particular interest to specialists in the fields of computing, Quantum Mechanics and encryption, for a couple of reasons. Firstly, because the algorithm was written not to run on a classical computer (like most published algorithms were) but on a Quantum computer, and secondly, because it had huge ramifications for security across the entire Internet. This was the paper to start all of the debate around whether Quantum Computers would be able to crush the encryption the Internet had relied for two decades. The algorithm proposed by Shor, when running on a Quantum computer, would be able to factor an integer in "polynomial time" (10) (Shor's Algorithm, 2018). Essentially, this means that the algorithm would be far, far faster and more efficient than any algorithm run on any classical machine at factoring integers (reducing a large number, eg: 735, down into just the prime numbers that make it up, in the case of 735, 1x3x5x7x7). Unfortunately, for the future of encryption, the one-way functions (see above) that we used to build our cryptosystems rely on factorisation, as classical computers are not very good at it, so take a very long time to break keys. Quantum Computers on the other hand, utilizing Shor's algorithm, may be able to reduce the time taken to break RSA's standard 1024 bit or greater encryption from millions of years to minutes.

However, this may not spell the end for the Public Key encryption of the Internet, (the main Public Key encryption scheme being RSA), as there are a number of arguments to be made against Shor's algorithm. Firstly, one 2017 paper (from pointed out that RSA might not actually be totally unsalvageable after the advent of Quantum, essentially claiming that the RSA algorithm is faster still than Quantum Computers (even when assuming Quantum Computers are far faster than predicted) and especially so when larger bit keys are involved (think 16,348 bits). The paper, written by four leading researchers (ranging from the Department of Mathematics and Computer Science to the University of Illinois, Chicago), proposed parameters for RSA encryption such as key generation, encryption, verification, decryption that are "feasible on today's computers while all known attacks are infeasible, even assuming highly scalable Quantum Computers" (11) (Daniel J. Bernstein, 2017). Not only does the recency of the paper help make its case all the more poignant, but no one has yet mounted a sufficient argument against it (although this also may be to do with its recency). Furthermore, (as mentioned in my section on Emerging Supercomputers), Quantum Computers still have a long way to go before we can use them to crack encryption quickly. The main issue to overcome is decoherence (see section 1), where the Quantum properties that make allow the Quantum Computers to vastly out-perform classical computers simply don't happen. This means that not only can current Quantum Computers operate for only a few seconds before having to be stopped and read (or "measured"), but they also need to be

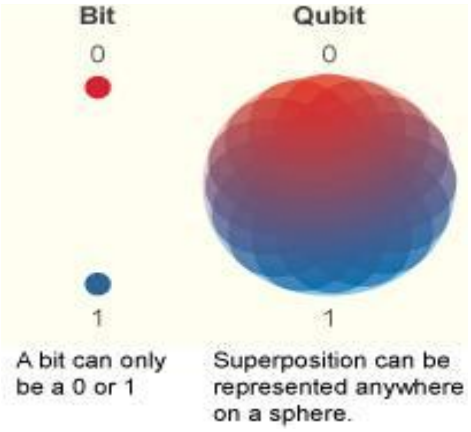
kept at a cool minus 270 degrees Celsius (some require to be cooled within 20 millikevins above absolute zero (3) (Quantum Computing, 2018)). On top of that, not only are Quantum Computers currently very much specific use machines, built to solve specific problems rather than "general use computers" that are built to solve any input (like classical computers), but the Quantum Computers currently in the labs of Google, Intel and IBM utilize too few Qubits to come close to being able to run Shor's algorithm and achieve factorisation speeds anywhere close to those necessary to be a real threat to encryption. Indeed, on March 9th of this year, Google unveiled Bristlecone, a Quantum Computing chip with 72 Qubits (despite being a new record, it's not really enough in terms of the numbers needed to perform algorithms such as Shor's to the speed needed), along with an announcement (made by John Martinis, a physicist who is heading up the collaboration between UCSB and Google to build a Quantum computer) that they expected to achieve Quantum supremacy using the new chip in "just a few months" (12) (Knight, 2018). Although these are huge steps forward in terms of the development of Quantum Computers, they will need to go much further than they have in order to pose the level threat to online encryption that people are worried about.

Yet despite the apparent shortcomings of the expectations that have already been made of Quantum Computers, from the research I've conducted for this dissertation (from newspapers to journals to papers to videos), the general consensus seems to be that *it is only a matter of time.* Quantum Computers have already come a very long way in the short time that people and companies have been working on them, with estimates stating that we will be seeing the first commercial Quantum Computers anywhere between 5 years' time (which seems a bit optimistic) to NIST's (the National Institute of Standards and Technology, USA, an organisation that predicts future trends and manages online standards) predicted 10 years ("NIST estimates the first cryptographically relevant Quantum computer could be built by 2030 for a cost of about one billion US dollars" (13) (Quantum-safe cryptography, 2016)). Regardless of whether the first commercially available or first general-purpose Quantum Computers are able to crack RSA or not, it is almost certain that at some point in the future they will be able to. After the first Quantum Computers are release to the public, researchers and computer scientists will have so much more data to work with, that the Quantum Computers will only advance more rapidly. Besides, some governments (such as the USA and Russia) have a vested interest in being able to crack encrypted data of other countries citizens, or even their own citizens. Of the 47 companies that Wikipedia lists as being involved in the development of Quantum Computers or Quantum communication, 19 of them are based in the US, and it is also highly likely that various US government departments have sunk their own money into developing Quantum Computing

capabilities (as mentioned before, most likely with the purpose of being able to break RSA and other Internet encryption systems). The threat posed to Internet security by Quantum Computers is increasingly becoming a matter of "when" not "if".

The Solution: Quantum Cryptography and More Secure Cryptosystems

So what can we do about the looming issue of Quantum Computers breaking our security? Fortunately, the answer is already here, in the form of the newly emerging field of Quantum Cryptography. If we were to use Quantum cryptography, then Internet cryptosystems will be able to utilize the same Quantum properties that give Quantum Computers their power, essentially "fighting Quantum with Quantum". There are already some proposed Quantum cryptosystems, most of which make use of the fact that Quantum particles are in a superposition (for a qubit, this means that they are neither a one or a zero, but both at the same time, inset right (Collins, 2017)(21)) until measured, at which point they collapse into one state (in this



Representation of a qubit in superposition.

example, the qubit would become either a zero or a one only after it was measured). This means that you cannot know which state a qubit is in before measuring it. Because cryptosystems such as these rely on fundamental laws of nature, instead of manipulating numbers, many of the already proposed Quantum cryptosystems (such as BB84, a Quantum key distribution method proposed a lot earlier, in 1984, and recently proven in a 2001 by leading expert in Quantum physics and Computer Science Peter Shor in another paper (14) (Shor, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, 2001)), they are far, far harder to crack than classical encryption, if even possible to crack. This gives them security not just against Quantum machines, but also other future threats made by classic computers (see next section), that current classical cryptosystems may not be able to handle. This makes Quantum key distribution a superior choice over classic key distribution schemes and cryptosystems. As Quantum Computers come closer and closer to our grasp, it becomes more and more vital that the

infrastructure of the Internet should make a universal move from classic cryptography to Quantum key distribution schemes. With the way Quantum-computing technology is heading and the rate at which it is advancing, a universal switch to Quantum key distribution is the best way to ensure the security of the Internet in the future.

The advent of Quantum cryptography as the system to distribute keys over the Internet is great, but there are some other points we will need to consider in order to achieve a universal movement from classic cryptosystems (ie: pre-Quantum) online, to Quantum cryptosystems. Most notably, governments around the world will need to undertake serious work on the cables that currently carry the Internet, in order to modify and change them so that they can actually carry the Qubits that are required for Quantum cryptosystems to work. This will cost time, money and resources; it will most probably be very expensive, and require a lot of man-hours. Indeed there are currently some experimental and prototype networks built for carrying Qubits between computers, but much further testing will need to be done before these networks and cables are able to handle anywhere near the amount of information that passes through our current networks on a daily basis, or at a speed that makes downloading files and streaming services from the Internet feasible. But developing technology like this is essential to provide security to the Internet in the future; it seems to not only be our best defence to hold out against Quantum Computers, but our only long-term plan to deal with the rise of Quantum Computing, and to still provide secure encryption as Quantum Computers become better and better.

Other Issues facing encryption: Exploits, and Smarter Hackers

Although there is very little new Cyberspace technology that is promising to match Quantum Computing in terms of threat to encryption, the threats to encryption outside of Quantum Computers cannot be overlooked, especially when considering the future of security on the Internet. Despite the fact that no classical attack (Cyber-attack made using a classical computer) has yet managed to totally and consistently defeat RSA, recent hacking trends are moving towards larger and more damaging attacks against businesses and government facilities, more data bank breaches leaking millions of personal files, and most recently, undermining electoral confidence in other countries and influencing important votes. These all have been, and will be (for the short-term future) accomplished using classical computers. It is important that in the face of the threat of Quantum we do not underestimate the power of the computers that we have already been developing for half a century. Broadly, the issues that our cryptosystems will have to deal with outside of Quantum can be split into two categories: changes and advances in classical computing technology, and new trends in hacking behaviour.

Technological advances in classical computing may not have, as much of an impact as advances in Quantum Computing will on encryption, but still cannot be ignored. In fact, many changes and updates to systems and software can actually have the unintended effect of creating new exploits or can (if the development wasn't done properly) give hackers new backdoors to exploit. In May 2017, the WannaCry virus (defined as a "cryptoworm" by Wikipedia (15) (WannaCry Ransomeware Attack, 2018), inset below (WannaCry Ransomeware Attack, 2018)) was discovered as the software was activated on over two hundred thousand systems across the world, including train companies in Europe, the NHS in the UK and Boeing in the US. Most of these companies immediately ground to a halt as their files were encrypted and held as ransom against them for a payment in Bitcoin (15) (WannaCry Ransomeware Attack, 2018).

The screen victims of WannaCry virus were presented with demanding bitcoin payment for their encrypted files.

The outbreak lasted roughly 4 days, from the 12th to 15th of May, although the virus would have spread itself before this time. WannaCry was able to spread so far and cause such widespread damage by exploiting an issue with the Windows Server Message Block (SMB), which is the "transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services" (16) (Islam, 2017), as reported by Fireeye, in a Cyber Security specialist blog. The exploit, released by Shadow Brokers (a group of hackers who in 2013 successfully stole a large amount of data from the NSA, and have been publishing the exploits found within ever since) one month prior, called "EternalBlue" allowed for remote execution of code, meaning that any code sent onto a network could be left alone to spread, until the whole network was compromised and could be brought to a standstill with one command from anywhere in the world.

As both hardware and software, companies continue to push updates to their products, it is highly likely that more of these exploits will emerge, potentially leading to other world-wide

hacks. This is the main issue with technological advances that they will create issues that can be exploited by hacking groups, not the actual advances themselves. Despite the fact that computer chip design and architecture is getting better and better, classical computers are still nowhere near powerful enough to do any sort of damage to RSA and other commonly used cryptosystems, and instead have to rely on exploits such as EternalBlue. This is especially true as we come to reach the end of Moore's Law (a law stating that the overall computing power of computers will double every two years (17) (Moore's Law, n.d.)) within the next couple of decades, and chip designs are running into issues, such as where the grooves on circuit boards are too close together, allowing electrons to Quantum tunnel between them, messing up the computer's operations.

Other issues facing the future security of the Internet revolve around the hackers themselves. Hacking groups are now getting state sponsoring and even training in some countries. Russia has its own "troll factory", and although it supposedly does not get involved with hacking, it does hire people to spread division over the Internet (most famously affecting the 2016 US presidential election (18) (Myers, 2018)), as reported by Jolie Myers, who interviewed a Russian anti-Putin activist who had had past experience working inside the troll factory. More alarmingly is that in China, in order to create a "Cyber legion" has been recruiting children, from a fairly young age, who are skilled at using computers and training them with hacking skills and penetration abilities. Furthermore, the current Chinese president, Xi Jinping aims to build "four to six world-famous Cyber Security schools" within 10 years (19) (Hunt, 2017), prompting criticism that China aims to build a "Cyber Army". However, disregarding the political motivation behind training hackers, equipping large numbers of people with the ability to penetrate other systems and steal data from supposedly secure systems does not bode well for the future security of the Internet.

Conclusion:

As I have outlined over the course of these 5 paragraphs, there are many challenges for us to meet that Quantum Computers *will* come to pose to encryption and Internet security. Although some people still defend RSA (and our current Public Key Internet cryptosystems in general), suggesting that we can easily modify our current technology to withstand Quantum Computers, the development of Quantum Computers is only going to increase in pace. At the same time, development of classical computers will start to slow down, as we run into the same fundamental laws of nature that Quantum Computers take advantage of, yet in the case of classical computers, these laws of nature pose a huge problem instead of giving the computers

tremendous power. Regardless of how well a reworked version of RSA might be able to do against the foreseeable Quantum Computers, nothing will be able to properly predict how powerful the first general purpose Quantum Computing machines might be, and even if they are in line with expectations (or fall short) it is almost certain that within another 10 years they will be able to surpass most expectations made of them, much in the same way that the technology of classical computers progressed hugely just from 1995 to 2005. As I mentioned for the main point of my third section: *it is only a matter of time* before our current standards and systems of encryption (or the best we can do with what we currently have) is breached completely. The only way to protect our security is to transition to an entirely different system; that of Quantum cryptography. It will not be easy to undertake this transformation to a new system, but it is necessary for the security of the Internet. Perhaps not all the cables will need to be dug up and re-laid. If we can find a way of expressing Qubits in classical bits (even if it takes several hundred or thousand bits to write one qubit) , then we can avoid having to re-lay some of the harder cables to reach, such as the undersea cables between continents, by using relay stations to switch the data from Qubits to classical bits. Quantum cryptography will be able to fight both fronts of the threats to encryption. Classical computers will not only be unable to do anywhere near the necessary number of operations per second to keep up with Quantum servers and computers, let alone even similar calculations to Quantum Computers, simply because of the differences in the way the two systems operate. This will keep a new, Quantum cryptosystem (or key distribution system), secure from any classical threats that might emerge. Furthermore (as I mentioned in my fourth section), Quantum encryption systems rely on fundamental laws of nature rather than manipulation of numbers, in the most secure cases, this results in the actual keys themselves being impossible to crack (because the states of the Qubits physically cannot be known until they are measured, yet doing so would disrupt the system in a detectable way, giving the server warning to re-generate and redistribute the key). The implementation of such a system may be difficult and expensive, but current standards of encryption will not be able to stand up to the future threat, most notably from Quantum Computers, and the only way to ensure the continued security of the Internet is to make the universal move to Quantum systems of encryption and key distribution.

Bibliography:

56-bit Encryption. (2017, 8). Retrieved from Wikipedia. (8)

Arthur, C. (2013, 9). *How Internet Encryption Works*. Retrieved from Guardian. (1)

Caesar Cipher. (2018, 4). Retrieved from Wikipedia. (4)

Collins, C. W. (2017, 6 28). *Quantum Computers: How Google & NASA are pushing Artificial Intelligence to its limit*. Retrieved from UMassAmherst: https://blogs.umass.edu/Techbytes/2017/06/28/quantum-computers-how-google-nasa-are-pushing-artificial-intelligence-to-its-limit/ (21)

Corera, G. (2015). *Intercept.* (5)

Daniel J. Bernstein, N. H. (2017, 4). Post-quantum RSA. (11)

Encryption. (2018, 4). Retrieved from Wikipedia. (2)

Foundation of Coding: Block Ciphers, Algebra, and Arithmetic. (n.d.). Retrieved from Apprize.

Foundations of Coding: Compression, Encryption, Error Correction. (2015). Retrieved from Apprize. (20)

History of Encryption. (2012, 5). Retrieved from Visually. (6)

History of the Internet. (2018, 4). Retrieved from Wikipedia. (7)

Hunt, T. (2017, 8). *China pumping MILLIONS into developing 'cyber army with world famous web security schools'*. Retrieved from Express. (19)

Islam, A. (2017, 5). *SMB Exploited: WannaCry Use of "EternalBlue"*. Retrieved from FireEye. (16)

Knight, M. G. (2018, 3). *Google thinks it's close to "quantum supremacy." Here's what that really means.* Retrieved from MIT Technology Review. (12)

Moore's Law. (n.d.). Retrieved from Moore's law. (17)

Myers, J. (2018, 3). *Meet The Activist Who Uncovered The Russian Troll Factory Named In The Mueller Probe*. Retrieved from Parallels. (18)

Quantum Computing. (2018, 4). Retrieved from Wikipedia. (3)

Quantum-safe cryptography. (2016, 11). Retrieved from National Cyber Security Centre. (13)

Shor, P. W. (1995, 8). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. (9)

Shor, P. W. (2001, 3). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. (14)

Shor's Algorithm. (2018, 4). Retrieved from Wikipedia. (10)

WannaCry Ransomeware Attack. (2018, 4). Retrieved from Wikipedia. (15)