# Progression of Cryptography

Patrick Mc Connell

13507173

Review article for CS275 2015

B.Sc. Computer Science and Software Engineering

Maynooth University

National University of Ireland Maynooth

Department of Computer Science

National University of Ireland, Maynooth

Co. Kildare

Ireland

*A review article was submitted in partial fulfillment of the requirements for the continuous assessment of the Directed Reading in CSSE module CS275 on the B.Sc. Computer Science and Software Engineering*

Lecturer: Mr. Joseph Duffin

# Declaration

I hereby certify that this material, which I now submit for assessment on the program of study as part of the continuous assessment for module CS275, is *entirely* my own work and has not been taken from the work of others - save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: Patrick Mc Connell Date: 30th April, 2015

# Acknowledgements

I would like to thank Joseph Duffin for his help throughout this project and many resources he identified to be used. I would like to thank my class for helping me define my idea and structure my topic into coherent topics.

# Abstract:

Cryptography is the basis of all modern information exchanges. Anybody who has needed to send an email or has used social media has come across it in some shape or form without even knowing it. With growing computational power comes a greater threat to our delicate information. Cryptography is a field of great importance and is an every growing part in society. It is important that we can discuss such and advanced topic in terms of how it effects us as the main daily user if it. In this review aim to achieve an overview of cryptography methods used currently, purposed in the future and the advancements made through the years that has led to the current lifestyle and security we have achieved. I also want to examine the current methodology used, its flaws and possible rectifications purposed by masters in the field.

# Introduction:

In this review I want to define and describe how the development of modern methods in cryptography may have a massive effect in our everyday lives from an internet security perspective. “We can define Cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it”. It plays a massive role in our modern world with huge data-centres communicating together constantly.

The databases of information I used to carry out this review consists of but was not limited to Google Scholar, IEEE Xplore, Citeseer and Science Direct. For any abstract information I used in my review, I tried to use the most up to date sources I could find to improve the reliability of the used facts.

The history of cryptography has paved the way for huge advancements in the modern day and may hold clues to developing the current methods of cryptography further. These include but are not limited to elliptical curve cryptography which has been in the limelight in recent times.

Although the field of modern cryptography looks promising, it has its limitations. There has been little evidence to suggest that one way algorithms such as the discrete logarithm problem or the generation of random prime factors is possible to be solved in polynomial time, rendering it infeasible. We have not yet found a fundamental flaw in these methods that would allow us to process the huge inputs without the use of a quantum computer.

The importance of modern cryptography is now more than ever of great importance. With the number of users exchanging delicate information rapidly the growing the need for more and more secure channels also grows. With the computational power of computers exponentially growing it may be the case that in the future it will be possible for people to hack others information in real time.

# History:

### *The Enigma machines role:*

The unambiguous history of cryptography's development is something that is often overlooked although it has developed the world as it is today. Cryptography was first seen as a power during the 1930's. During this period machines such as the enigma machines development was in motion. The Enigma machine was an advanced electro-mechanical cipher machine developed in Germany after World War 1. "The Enigma machine was used by all branches of the German military as their main device for secure wireless communications until the end of World War 2". It used the idea that only users with the booklet for that day could adjust the rotors to the right specification for that day. This allowed only the people who were intended to read the cipher to decode the message. "It was created by Arthur Scherbius a German engineer, in the hope of interesting commercial companies in secure communications". This proved to be both an advantage and a hindrance which ultimately changed the course of the war.

### *Modern methods:*

With this in mind, it is important to recognize the developments it led to and the new methods with increased complexity it produced. In 1984, Taher Elgamal came up with an algorithm based on a one-way function. His algorithms functionality depends on the user's ability to decipher the discrete logarithm problem. The problem faced is that it is easy to exchange a cipher given the private key, but without it, there is no way to easily predict the input value needed to decipher

the formulae G^x MOD P. Here x the power of G is unknown to the hacker, and the modulus creates a trap door which means you cannot yet decrypt what number to put in to get the desired output. This leads to an incremental check of each input which takes exponential amounts of time, meaning that it is infeasible to try for exceedingly large numbers.

Another method that is being used vastly is the RSA method of encryption. First recognized as the work of by 3 Cryptographers Ron Rivest, Abi Shamir and Leonard Adelman, it uses huge prime numbers that are exceptionally hard to decompose into its prime factors. As the size of the numbers grow, the decisions to decompose the number into its fundamental prime factors grows. Like the discrete logarithm problem, its security is defined in the difficulty to find an easier way to solve the problem than incrementally breaking it down into a smaller sample size.

There is however, other variants of the RSA algorithm such as Pell's algorithm, dual RSA and n prime RSA algorithms which are based on the same idea. In this Pell's RSA, an efficient public key cryptosystem has been implemented based on Pell's equation which is shown by using different key parameters. From the security analysis, the evaluation of proposed RSA is measured with standard RSA. "Through these outcomes, it has been noticed that there is tremendous variations on Pell's key generation with normal RSA which prevents the attack against Wiener's Theorem"

## *Current development:*

Now in the current era, there is a lot of promise in the topic of elliptical-curve cryptography. "Elliptic Curve Cryptography is an approach to public-key cryptography, based on elliptic curves

over finite fields. The technique was first proposed individually by Neal Koblitz and Victor Miller in 1985". This type of cryptography is based on the discrete logarithm problem and is known to be an NP-intermediate problem. It defines a finite area on a graph and a fixed curve in this region. It uses this to define points that are on the curve. From this we are able to a number that is order of the point, and c must divide the order of the curve. With this, and a good chosen point to produce a large prime number it is able to compute the same expected security in 2 to the power of "N" divided by 2. This means the same security is achieved with smaller selected primes than with the RSA's factorization of large prime's method.

# Limitations:

*Classical VS quantum cryptography:*

Although the field of modern cryptography has mad leaps and bounds in the right direction, it has to deal with more and more huge inputs that are becoming infeasible for the modern computer. The purposed answer to this is quantum cryptography. “Quantum cryptography was first proposed in 1984 by Brennet and Brassard based on the No-Cloning theorem”. A great advantage of cryptography through quantum cryptography is that the eavesdropper is detected in the process. If someone tries to eavesdrop it changes the state of photons polarization thus, it is an indication that the line has been tapped. In saying this, quantum cryptography has no yet become feasible in many ways. Recently, it was recorded that a quantum can transfer data a rate of 16 bits a second and can only reach a distance of 250km compared to satellites being 36000 km from the earth’s surface. This is not feasible with the likes of plug in and play devices becoming more popular.

Another limitation for quantum cryptography is that we are unable to realistically identify if the information is authentic. It is known that the use of algorithms is not easily implemented in quantum cryptography. Thus, the 3 main algorithms consisting of key generation, digital signature and key verification are absent in this process. Without this, the source of the information received is unreliable and could be subject to change.

*Quantum cryptography accessibility:*

Another way in which it has its limitations is how easily the information could be messed with. For example, if a hacker was able to access the fiber cable they could easily change the entire data structure meaning the wrong message is received. Just a paper clip is all that is needed." A paper clip when pinched onto the fiber causes the change in refractive index at that point leading to change in polarization which ultimately leads to wrong of interpretation of data".

Also, as above, it is easy for the data to be changed through a bit error rate. This is a few percentages higher than in classical cryptography and means it is seriously impractical if the message is lost in transmission and indecipherable as a result. There is a countermeasure called CASCADE which has been put in as an error correction protocol. This however, has its drawbacks. The main problem with this is that it is susceptible to attacks and may possibly leak bits in the private key, meaning it would be much easier to decode.

# Importance of cryptography today:

### *Devices:*

Cryptography has a larger and larger part to play in our modern society. With the amount of devices capable of sending and receiving information exponentially growing, it is important that our security measure is up to scratch. For instance, “in 2015 the amount of accounts used by consumers was 2,586 million and the amount of emails sent and received daily was 205 Billion”. With this in mind, it is clear that cryptography is a vital part of everyday society.

### *Information channels:*

Without cryptography, the world would possibly fall into a state of chaos. Without it, it would easily be possible for a well-informed person to hack into a nuclear launching facility or into the power grid of a city causing disruption to millions of people. Also without cryptography there would be no secure exchange of credit card details leading to anyone being able to access, use and distribute your personal information on the black market and cause many more problems.

### *Growing E-commerce:*

The use of the internet to do business between multi-national companies is growing. Many

companies have begun to adapt to the changing world and use a function known as cloud computing. It is suggested that “the percentage of U.S. small businesses using cloud computing is expected to more than double during the next six years, from 37 percent to nearly 80 percent”. This is a huge increase in online data holding. With this in mind, the amount of information available and accessible from our own homes has grown drastically. This is possibly a huge threat and is a jump in technology, which may not yet be able to be backed by efficient enough algorithms to ensure its safety.

# Conclusion:

As is evident from above, cryptography has a vital part to play in our modern society and shows promise in fields like elliptical curve based algorithms to maintain the high security and strength we know and rely on. It has come a long way from ciphers used in World War 2 such as that used in the enigma machine to the ciphers we commonly use today, namely the RSA factorization of large prime's algorithm. There is also a lot of promise from a quantum cryptography, although its security is not yet concrete enough to be used in a practical sense.

With this, it is easy to see modern cryptography methods as NP problems. This means there is no known way to compute a reliable answer in polynomial time, making it extremely difficult to dispute the need for new better methods.

From my research I can confidently suggest that for cryptography to progress further and stronger, a conversion to quantum cryptography is needed. If developments in quantum cryptography allow the commonly used algorithms to be implemented, as they are not currently available, it would mean for a faster, more concrete security system which could abort the exchange if too many bits of the private were leaked.

It is also evident that in the case of our current information channels that we will need to further develop a successful way of protecting delicate information which is sensitive enough to cause

an economic collapse or even the possibility of a new age war.

# Further recommendations:

From my limited knowledge of the field, I anticipate that the next step in this field is either in the promise of quantum or elliptical curve cryptography becoming more viable. If quantum cryptography becomes reliable enough to be used in a practical sense, it paves a whole new way and idea for security, based not on computational difficulty but on laws of physics. Also, if methods currently being discussed like the elliptical curve method make a break through to allowing computations of huge prime number based keys in polynomial time becomes achievable, the computational hardness of currently used algorithms of encryption will need to make a change to ensure security. I believe that further investigation into patterns in key generation from a given number. If memory wasn't finite, i believe that a possible solution would be to store the possible outcomes of a given public key, and have the algorithm be based on a look up function rather than an iteration of possible candidates for a solution. I believe the answer lies in not the computational power of modern computers, but in AI. If it were possible to have an AI that could learn like a human and anticipate the inputs to produce a valid outcome (private key generation in this case), it could lead to greater understandings of both AI and cryptography.

# References:

ekert, A. (1991, August 5). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 661-661.

Email Statistics Report , 20 15 - 201 9. (2015, March 1). Retrieved April 30, 2015, from http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

Kapoor, V., Sonny Abraham, V., & Singh, R. (2008). *Elliptic Curve Cryptography, 9*(20), 1-8. Retrieved April 29, 2015, from http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/abhishek3.pdf

Lycett, A. (n.d.). Enigma. Retrieved April 29, 2015, from http://www.bbc.co.uk/history/topics/enigma

Segar, C. (2013). Pell's RSA key generation and its security analysis. Retrieved April 29, 2015, from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6726659

Sharma, D. (2014). Quantum Cryptography: Pitfalls and Assets. *International Journal of Enhanced Research in Science Technology & Engineering, 3*(5), 27-30. Retrieved April 29, 2015, from http://www.erpublications.com/uploaded_files/download/download_17_05_2014_17_37_50.pdf

Vignesh, R.S, Sudharssun, S. , & Kumar, K.J.J.(2009). Limitations of Quantum & The Versatility of Classical Cryptography: A Comparative Study. 333-337

Winfrey, G. (2015, April 30). How the Cloud Will Transform Business by 2020. Retrieved April 30, 2015, from http://www.inc.com/graham-winfrey/why-the-cloud-will-transform-small-business-by-2020.html

(n.d.). Retrieved from http://www.2worldwar2.com/enigma.htm