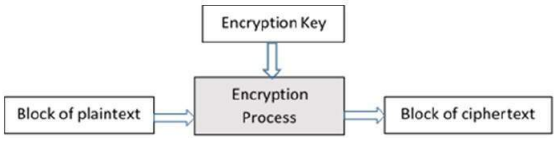
Literature review on Data Encryption, its algorithms, and the future of Data Encryption

Kevin Niland, *Computing in Software Development (Honours), GMIT*

***Abstract*—Data encryption is integral to many different areas in the computing world. Encryption is used to help protect sensitive data by changing it into a form only readable by a person or entity who has the decryption key. Vast amounts of personal information is managed online and stored in the cloud/servers. With computers becoming increasingly more and more powerful [CHANGE], so too comes the risk that peoples personal information can be accessed by an unauthorized party. As a result, several different algorithms and methods have emerged to prevent this. This paper will look at two of these algorithms that are in use today: Rivest–Shamir–Adleman (RSA) [10] and the Advanced Encryption Standard [4], which came about 23 years after RSA Encryption. In this paper, both of these algorithms are discussed at length in regards how they came about, their advantages and disadvantages, and some of their applications. This paper will also look at the future of data encryption and various methods that could feasibly be proposed as possible replacements for current algorithms and techniques.**

I. Introduction

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct decryption key. Encrypted data, also known as cipher text, appears scrambled or unreadable to a person or entity accessing it without permission. Decrypted data, also known as plain text, appears readable to a person or entity accessing it with permission. Currently, encryption is one of the most popular and effective data security methods used by organizations. A block cipher transforms plain text blocks of a fixed length n¡b to cipher text blocks of the same length under the influence of a cipher key k [13].



Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption. Asymmetric encryption came about after symmetric encryption, as an answer for secure communications with an emphasis on applications that could not have been satisfactorily handled by cryptographic techniques at the time [16].

A. History of Data Encryption

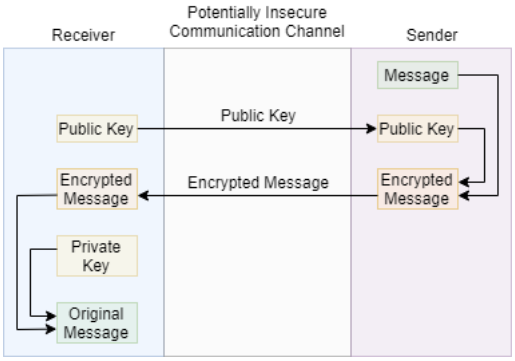
Data encryption, in one form or another, has existed for almost 3000 years. Circa 600 B.C. [1], Spartans use a device called a scytale to send secret messages during a battle. Circa 60 B.C., Julius Caesar invents a substitution cipher that shifts characters by three places. A becomes D, B becomes E, and so on. In 1553, Giovan Battista Bellaso envisions the first cipher to use a proper encryption key - an agreed-upon keyword that the recipient needs to know if he or she wants to decode the message. In 1795, Thomas Jefferson invented Jefferson's Wheel Cipher which was later used in the United States Army from 1923 to 1942. However, interestingly, the army never knew about Jefferson's invenetion. They simply re-invented it and called it the 'M-64' [12]. In 1854, Charles Wheatstone invents the Playfair Cipher, which encrypts pairs of letters instead of single ones and is therefore harder to crack [1].

B. Current Status of Data Encryption

Over time, however, the above mentioned methods have been proved to be insecure since eavesdropper - known as cryptanalysts - could exploit simple statistical features of the cipher text to easily recover the plain text and even the decryption key, allowing them to easily decypher any future messages using that system [19]. Modern computing technology has made it practical to use far more complex encryption algorithms that are harder to "break" by cryptanalysts. In parallel, cryptanalysts have adopted and developed this technology to improve their ability to break cryptosystems [9], [5], [20].

II. Asymmetric Encryption

Asymmetric encryption, also known as public-key encryption, is a form of data encryption where the encryption key (also called the public key) and the corresponding decryption key (also called the private key) are different. In this literature review, we will be looking at a specific asymmetric encryption algorithm, the Rivest–Shamir–Adleman algorithm. The Rivest-Shamir-Adleman (RSA) algorithm, was designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. The asymmetry of RSA is based on the practical difficulty of the factorization of the product of two large prime numbers, named "prime factorisation" [15]. Based on number theory, which is a block cipher system, it is one of the most widely known public key cryptosystems. It is used for key exchange, digitial signatures, or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. To generate the public keys (for encryption) and private keys (for decryption), it uses two prime numbers. The basic operation of the RSA algorithm goes as follows:



the Sender encrypts the message using the Receiver's public key. Once the message has been successfully transmitted to the Receiver, the Receiver can then decrypt the message using their own private key. The RSA operation(s) can be broken down into three broad steps: key generation, encryption, and decryption. In regards to this design, it has many flaws and is subsequently not suitable or preferred for commercial use. As discussed in Gurpreet Singh and Supriya's article, "***A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security***" [17]....

III. Symmetric Encryption

Symmetric encryption is a form of data encryption where the encryption key and the corresponding decryption key are the same. The persons or entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages. To discuss symmetric encryption, we must quickly look at the first standardized cipher which was the Data Encryption System (DES).

The Data Encryption Standard (DES) was first published in 1975, standardized in 1977 and ultimately withdrawn as the standard by the National Institute of Standards and Technology in 2001 [2]. It was the first publicly available cryptographic algorithm that was endorsed by the US. Government. As discussed in Miles E. Smid and Dennis K. Branstad's paper, "The Data Encryption Standard: Past and Future", the DES security controversy [18] forced security questions about how good is good enough and how long is long enough. This controversy came about due to DES' short key length of 56 bits, which was criticized from the beginning. Although this made it too insecure for most current applications (this is evidenced by the fact that it was cracked in 1997), it was highly influential in the advancement of modern cryptography and in the year 2000, it was replaced by the Advanced Encryption Standard (AES) which was found through a competition open to the public.

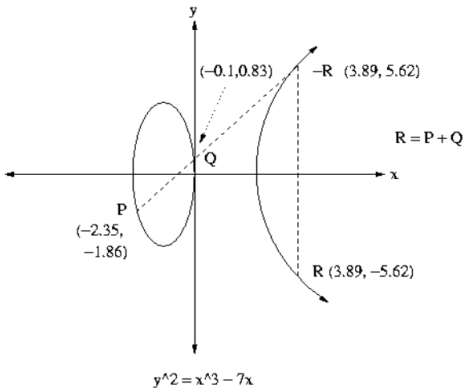
The Advanced Data Encryption Standard (AES), originally known as Rijndael, was developed by Vincent Rijmen and Joan Daemen. It was first announced in 2000 by NIST as the surprise winner [4] of its new Advanced Data Encryption Standard competition, and subsequently replaced DES in 2001 [17].... ADD MORE

IV. Future of Data Encryption and Possible Replacements of Existing Encryption Algorithms

There are several different techniques that could possibly be employed in the future to further enhance our ability to encrypt and decrypt our data. Some of these have been and still are being extensively researched and tested. Some examples include, but are not limited to: Elliptic Curve Cryptography (ECC), Quantum Computation, and a new data encryption algorithm based on the location of mobile users which has been given the name, "Location-Dependent Data Encryption Algorithm (LDEA)" has been also proposed.

A. *Elliptic Curve Cryptography (ECC)*

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. In Nicholas G. McDonald's research review, he discussed in brief Elliptic Curve Cryptography. As he stated, he states that Elliptic Curve Cryptography has technically already been invented but he considered it to be a future technique of cryptography because its advantages and disadvantages are not yet fully understood. In terms of encryption, ECC is an approach that utilizes the complex nature of elliptic curves in finite fields. A finite field (also called a Galois field, so named in honor of Évariste Galois, a French mathematician) in mathematics is a field that contains a finite number of elements. While RSA encryption and ECC typically use the same types of algorithms, the difference is that the numbers used are chosen from a finite field defined within an elliptic curve expression.



B. *Quantum Computation*

Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes). In Nicholas G. McDonald's research review, he also briefly discuss the possibility of using Quantum Computation as future method of data encryption. Quantum Computation is performed in a quantum computer or processor,

which is a processor that makes use of quantum mechanical phenomena, such as quantum superposition and quantum entanglement. Quantum superposition is a fundamental principle of quantum mechanics. Much like waves in classical physics, it states that any two (or more) quantum states can be added together - superimposes - and the result will be another valid quantum state. Using quantum logical qubit state, which is quantum superposition of the "basis states" 0 and 1 as an example, a superposition is where a qubit can be in the state 0 and 1 at the same time, contrary to a classical bit which can only be in the state corresponding to state 0 or the state corresponding to 1. Depending on the quantum design, each qubit can store a set number values simultaneously. Quantum computing is still in its infancy and, as a result, quantum processors manufactured today are very small and do not have the computational size that transistor processors have. Some fear that a successful and practical quantum computer would devastate the world's financial system by breaking every encryption system known - public-key cryptography relies on computer being slow to compute discrete logarithms and prime factorisation's.

C. *Location-Dependent Data Encryption Algorithm (LDEA)*

As proposed in Hsien-Chou Liao and Yun-Hsiang Chao's 2008 study, published in the Information Technology Journal [8], most of the data encryption technology is location-independent. That is, encrypted data can be decrypted anywhere. Encryption technology of today is unable to restrict the location of the decryption of data. Hsien-Chou Liao and Yun-Hsiang Chao proposed the idea of a location-dependent approach, named Location-Dependent Data Encryption Algorithm (LDEA). For this approach to work, a target latitude and longitude coordinate is determined firstly. The coordinate is then incorporated with a random key for data encryption. As a result, the receiver can only decrypt the cipher text when the coordinate acquired from the GPS receiver is matched with the target coordinate. A number of drawbacks to modern technology, such as GPS that would be used in this approach, renders LDEA difficult to implement well. The location of a mobile user is difficult to exactly match with the target coordinate due to current GPS receivers being inaccurate and inconsistent.

In Hatem Hamad and Souhir Elkourd's research paper, "Data encryption using the dynamic location and speed of mobile node", they proposed a simialar idea to that of the one proposed by Hsien-Chou Liao and Yun-Hsiang Chao in their paper. They proposed a method of key security where the receiver MN (Mobile Node) registers some coordinates and speed during the travel and thus can chart the course of movement [7]. Through this path, one can predict the next coordinate expected after a certain amount of time since the GPS receiver is inaccurate and inconsistent, depending on how many satellite signals are received, as mentioned in Hsien-Chou Liao and Yun-Hsiang Chao's paper. However, [8].

V. Conclusion

In this paper, we looked at modern methods and algorithms of data encryption, namely the Rivest–Shamir–Adleman (RSA) algorithm and the Advanced Encryption Standard (AES), briefly looking at the Data Encryption Standard (DES) which was highly influential in the advancement of modern crytography/encryption. This paper also looked at the future of data encryption, and reviewed possible methods and algorithms such as Elliptic Curve Cryptography (ECC), Quantum Computation, and Location-Dependent Data Encryption Algorithm (LDEA).

VI. TEMPORARY - REWORD AND ADD TO RELEVANT SECTIONS ABOVE

A. *Data Standard Standard (DES)*

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. Although its short key length is of 56 bits, criticized from the beginning, makes it too insecure for most current applications, it was highly influential in the advancement of modern cryptography. Developed in the early 1970s at IBM and adopted as the national standard in 1976 [4] and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. During this time the standard was revised three times: as FIPS-46-1 in 1988, as FIPS-46-2 in 1993 and as FIPS-46-3 in 1999. DES was an outcome of a call for primitives in 1974, which did not result in many serious candidates except for a predecessor of DES, Lucifer designed by IBM around 1971 [2]. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute-force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

B. *Advanced Encryption Standard (AES)*

The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

References

[1] *A brief history of encryption*. Apr. 2016. URL: https://www.gemalto.com/review/Pages/a-brief-history-of-encryption.aspx.

[2] Alex Biryukov and Christophe De Cannière. *Data encryption standard (DES)*. Springer-Boston, Massachusetts, 2005. ISBN: 9780387234731.

[3] G.R. Blakley and I. Borosh. "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages". In: *Computers Mathematics with Applications* 5.3 (1979), pp. 169–178. DOI: https://doi.org/10.1016/0898-1221(79)90039-7.

[4] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, Berlin, 2002. ISBN: 9783642076466.

[5] Niels Ferguson et al. *Improved Cryptanalysis of Rijndael*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 213–230. ISBN: 9783540447061. DOI: https://doi.org/10.1007/3-540-44706-7_15.

[6] K.A.G Fisher et al. "Quantum computing on encrypted data". In: *Nature Communications* 5.3074 (2014), pp. 1–7. DOI: https://doi.org/10.1038/ncomms4074.

[7] Hatem Hamad and Souhir Elkourd. "Data encryption using the dynamic location and speed of mobile node". In: *Journal Media and Communication Studies* 2.3 (Apr. 2010), pp. 67–75.

[8] Hsien-Chou Liao and Yun-Hsiang Chao. "A New Data Encryption Algorithm Based on the Location of Mobile Users". In: *Information Technology Journal* 7.1 (2008), pp. 63–69. DOI: https://scialert.net/abstract/?doi=itj.2008.63.69.

[9] Mitsuru Matsui. *Linear Cryptanalysis Method for DES Cipher*. Springer Berlin Heidelberg, 1994, pp. 386–397. ISBN: 9783540482857. DOI: https://doi.org/10.1007/3-540-48285-7_33.

[10] Evgeny Milanov. *The RSA Algorithm*. URL: https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf.

[11] Dag Arne Osvik et al. *Fast Software AES Encryption*. Lecture Notes in Computer Science. Springer-Berlin, Heidelberg, 2010, pp. 75–93. ISBN: 9783642138577.

[12] Roger A. Prichard. *History of Encryption*. Jan. 2002. URL: https://www.giac.org/paper/gsec/1555/history-encryption/102877.

[13] Davood Rezaeipour and Mohamad Rushdan Md Said. "The block cipher algorithm-properties, encryption efficiency analysis and security evaluation". In: *Advances and Applications in Mathematical Sciences* 4.2 (Jan. 2010), pp. 129–137.

[14] Rizky Riyaldhi, Rojali, and Aditya Kurniawan. "Improvement of Advanced Encryption Standard Algorithm With Shift Row and S.Box Modification Mapping in Mix Column". In: *Procedia Computer Science* 116 (2017), pp. 401–407. DOI: https://doi.org/10.1016/j.procs.2017.10.079.

[15] Yaroslav Sergeyev. "The Difficulty of Prime Factorization is a Consequence of the Positional Numeral System". In: *International Journal of Unconventional Computing* 12.5–6 (2016), pp. 453–463.

[16] Gustavus J. Simmons. "Symmetric and Asymmetric Encryption". In: *ACM Computing Surveys (CSUR)* 11.4 (Dec. 1979), pp. 305–330.

[17] Gurpreet Singh and Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security". In: *International Journal of Computer Application* 67.19 (2013), pp. 33–38.

[18] Miles E. Smid and Dennis K. Branstad. "Data Encryption Standard: past and future". In: *Proceedings of the IEEE* 76.5 (1988), pp. 550–559. DOI: https://doi.org/10.1109/5.4441.

[19] Ron Steinfield. *Encryption today: How safe is it really?* Mar. 2015. URL: http://theconversation.com/encryption-today-how-safe-is-it-really-37806.

[20] M.J. Wiener. "Cryptanalysis of short RSA secret exponents". In: *IEEE Transactions on Information Theory* 36.3 (1990), pp. 553–558. DOI: https://doi.org/10.1109/18.54902.

[2] [18] [9] [4] [11] [14] [5] [3] [10] [20] [17] [15] [13] [16] [12] [1] [19] [8] [6] [7]