CYBER SECURITY ON SATELLITES' DATA: EVALUATION OF CRYPTOGRAPHY ALGORITHMS

Joseph Hayes
Faculty Advisor: Dr. Chutima Boonthum-Denecke
Department of Computer Science, School of Science
Hampton University

ACKNOWLEDGEMENT
Dr. Chutima Boonthum-Denecke, my Professor and Faculty Advisor, deserves a special thank you for her unwavering support throughout the research process, as well as Dr. Jean Muhammad for drafting a letter of recommendation on my behalf. I'd also like to express my gratitude to Program Specialist Jan Dotzauer for providing me with this incredible opportunity.

I. Abstract

With a high quantity of people using the web every day and sending data across the internet, it brings a risk of personal/private information being stolen or damaged. I will briefly discuss two solutions to the vulnerability of data transfer: (i) updating security requirements for the specified organization and (ii) implementing a strong encryption algorithm for every single piece of data that is being transferred. The encryption solution will cover (a) quantum cryptography, (b) mathematical cryptography, © Advanced Encryption Standard (AES), (d) Triple Data Encryption Standard (TDES), (e) Rivest-Shamir-Adleman (RSA), (f) Blowfish, and (g) Twofish. The evaluation and analysis of AES, TDES, RSA, Blowfish, and Twofish spanning data package sizes from 15 to 10,000 characters with various ranges to efficiency. AES Encryption overall is the better algorithm with its substitution-permutation network, a Rijndael's variant with fixed block size and key sizes. However, Blowfish and Twofish are better with flexibility in lower block lengths. RSA Encryption is great for security; however, it was the slowest algorithm due to larger block lengths. In summary, each encryption algorithm has its benefit depending on the amount of data and security measures.

II. Introduction

With the increased use of technology, Cyber Security is more important than ever. With that said, there are numerous methods available to prevent or lessen the dangers of cyber assaults, both from a company's perspective with financing for the best security and in collaboration with the US government when transferring . Finding the optimal algorithm for public, private, and commercial data that is both efficient in software and hardware implementations that keeps the most sensitive information on a heavy duty lock when being transported from one location to another is one approach that I will be pursuing in this research.

III. Data Usage

We don't know it, but we transfer so much data everyday effortlessly while we're utilizing services, communication, the internet and social media. More than fifty percent of the web queries over the internet are searched using smartphones. It is estimated that more than over four billion people all across the globe are connected to the internet. The most popular search engine, Google, processes almost five million searches every single second and six billion searches per day. There are over one hundred and eighty million emails sent across the globe and there are over 4 million videos that are streamed over youtube every minute. With the increase in the popularity and easy accessibility of the

internet, the customers' digital footprints over the internet have accelerated. It is believed that over 2.5 quintillion bytes, or 2.5 e+9 gigabytes of data is created every day and is still increasing [7]. A lot of the data that is being transferred and shared are all possible through satellites, which are self-contained communication systems that contain the ability to receive signals from Earth and retransmit the signals back. Mobile phone networks, GPS technologies, a myriad of IoT devices and even electrical grids and other power suppliers regularly rely on satellites to keep their operations going. Any damage inflicted in the satellite sector can have a ripple effect, leading to heavy financial losses and/or compromised data in other areas [4].

IV. Vulnerability and weaknesses

With the increase of the digitized critical infrastructure, it makes the transferring of data more vulnerable to cyber attacks. This includes the usage of old and outdated space systems, regardless of cyber security being deemed top priority, costly cyber protection and hard coded credentials that are used by planes, ships and the military. These cyber vulnerabilities pose a major threat not only to space-based assets, but also to key infrastructure on the ground. These dangers could obstruct global economic progress and, by implication, international security if they are not addressed. To make matters worse, more countries and commercial actors have acquired and deployed counter-space weapons in novel applications, posing a larger existential danger to important space assets[13]. The proper solution towards these current issues are to communicate security requirements for the specified organization, and to implement stronger encryption for every single piece of data, specifically the data that is being transferred between satellites.

V. Encryption

With the process of encryption, the data that you share will be encoded, or converted into a format which is unreadable. When the individual on the receiving end has obtained the data, it will then decode and biome readable, but only to that said recipient. This process is only possible due to a digital key that's needed to decode the data. When you send information or data to someone else over the internet, it goes through a succession of network equipment located all over the world, all of which are part of the public internet network. Because your data travels through the public internet, there is a danger that it will be hacked. Installing appropriate software or hardware that ensures a secure transfer of your shared data or information can help you avoid such a vulnerability. This is how encryption works [1]. The cryptography and encryption that will be the main focus of this research is Quantum Cryptography, Mathematical Cryptography, AES, Triple DES, RSA, Blowfish and Twofish encryption. There are three encryption levels that are executed: plain text, encrypted text (or ciphertext), and decrypted text (which is the same as plain text). There are two encryption keys that connect with the different types of encryptions and how they operate: Symmetric and Asymmetric.

Symmetric Encryption

Symmetric works more on a singular private key, so it's faster than asymmetric encryption. During the process of symmetric encryption, the sender has to share the private key with the receiver in order to access the information/data.

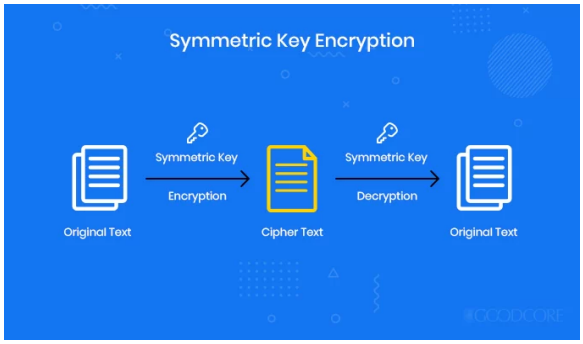

Fig. 1 Model of symmetric key encryption[1]

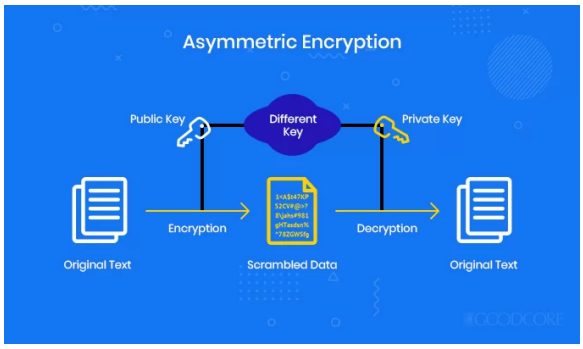

Fig. 2 Model of asymmetric key encryption[1]

Asymmetric Encryption

One public key and one private key are used in this encryption method. Anyone has access to the public key. The private key, on the other hand, must remain a secret key since you'll use a public key to encrypt your data or communication and a private key to decrypt it. Consider a circumstance in which you have two locks on a box containing confidential information. One of those two locks is equipped with a master key that anyone can use. The second key, on the other hand, is solely with you and a companion with whom you must share the box. You enlist the assistance of another individual to deliver the package to your acquaintance with the assistance of another individual. He tries to open it, but because he has the master key, he can only get through one lock. With no luck, he delivers the package to your acquaintance, who can access the information you supplied with the use of a second key [1]. Because this encryption approach uses two keys, any algorithm based on it will be deemed the most secure because it assures high levels of security. No one has been able to crack asymmetric key encryption until now.

Quantum Cryptography

By the extension of encryption, Quantum Cryptography encrypts data and transmits it in an unhackable manner using quantum mechanics principles. One thing about Quantum Cryptography compared to Mathematical Cryptography is that it's more complexed due to those mechanics since the particles that make up the universe are fundamentally unpredictable, and they can exist in multiple places or states of existence at the same time, in one of two quantum states, photons are generated at random, a quantum property cannot be measured without causing it to change or be disturbed, and some quantum attributes of a particle can be cloned, but not the entire particle. To break down the process of Quantum Cryptography and how it works, Photons are sent via a filter (or polarizer) that gives them one of four polarizations and bit designations: vertical (one bit), horizontal (zero bit), 45 degree right (one bit), or 45 degree left (one bit) (Zero bit). The photons are sent to a receiver, which "reads" the polarization of each photon using two beam splitters (horizontal/vertical and diagonal). The receiver must estimate which beam splitter to utilize for each photon because it does not know which to use. After the stream of photons has been sent, the receiver informs the sender of which beam splitter was used for each photon in the sequence it was sent, and the sender matches this information to the polarizer sequence used to convey the key[2].

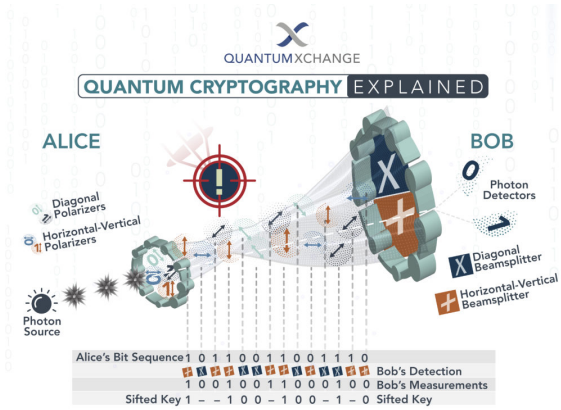

Fig. 3 Quantum Cryptography Diagram[2]

Mathematical Cryptography

The science of using mathematics to encrypt data is known as cryptography. It entails storing confidential information with a key that only authorized individuals have access to. It's difficult to tell what the original is without deciphering the encryption. Cryptography is crucial for understanding the mathematics side of encrypting and decrypting data, and cryptanalysis is vital for understanding the mathematics side of encrypting and decrypting data. The use of mathematical techniques, pattern recognition, analytical thinking, determination, and a little bit of luck are all used in cryptanalysis [11]. Cryptanalysts are people who look for flaws in systems and attack them. The strength of Mathematical Cryptography is solely based on the resources given and the amount of time it would take to recover the plaintext while the outcome of the Cryptography should be the same. Even though this form of Cryptography has advanced over the span of 100 years, In today's world, this is not the type of mathematical cryptography that can protect data due to how simplified it is compared to the process Quantum Cryptography and the mechanics that are instilled in it.

Triple DES

The Triple Data Encryption Algorithm, sometimes known as Triple-DES, is a symmetric encryption algorithm. It is a more advanced version of the DES block cipher, which previously had a key size of 56 bits. TDES, on the other hand, encrypts data three times with a 56-bit key, resulting in a 168-bit key. When encrypting data, it works in three stages: it encrypts, decrypts, then re-encrypts. The decryption phase is the same. It is much slower than other methods of encryption since it encrypts three times. Not only that, but it also encrypts data in small block lengths, making decryption relatively simple throughout the encryption process. As a result, there is a greater chance of data theft. It was, nevertheless, the most suggested and commonly used method before other modified types of encryptions arose [1]. Despite the fact that it is being phased out, many financial and business organizations continue to utilize this sort of encryption to protect their data.

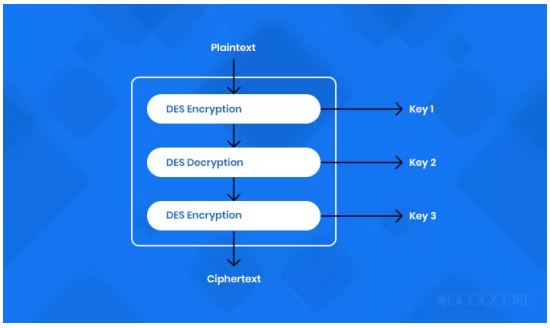

Fig. 4 Triple DES encryption model[1]

AES

The Advanced Encryption Standard (AES) uses the Rijndael algorithm for symmetric encryption. It encrypts one fixed-size block at a time using block cipher. It works with 128-bit or 192-bit keys, but it may be extended to 256-bit keys. Different rounds are used to encrypt each bit. For example, 128-bit has ten rounds, 192-bit has twelve rounds, and so on [1]. Because it was developed by the US National Institute of Standards and Technology, it is regarded as one of the greatest encryption algorithms. Because it is based on a single private key, it is also one of the most secure methods of encryption.

RSA

The Rivest–Shamir–Adleman (RSA) cipher is an asymmetric cipher that uses two keys for encryption and decryption: a public key for encryption and a private key for decryption. It operates on a 1024-bit key length and can be extended up to 2048-bit key length, making it the best encryption technique. This indicates that the encryption process grows slower as the key size increases. It is believed to be one of the strongest encryption types due to its bigger key size. Because it is the most secure encryption technique available, it is also used as an encryption standard for data shared over the internet. Because of the length of the keys it uses, RSA gives hackers a hard time when compared to other methods of encryption.

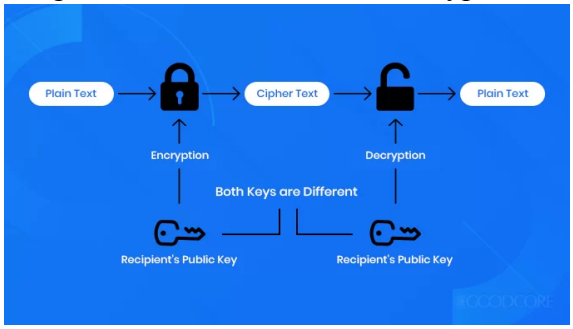

Fig. 5 RSA encryption model[1]

Blowfish

Blowfish is a symmetric block cipher that works with a configurable key length ranging from 32 bits to 448 bits, and was designed to replace DES. Because it is a block cipher, when encrypting and decrypting data or a message, it divides it into fixed 64-bit blocks. It was created to be quick to use and is available to everyone as free public encryption software[1]. It does not have a patent or a license. It has been thoroughly tested for speed, efficiency, and security as a public encryption platform. No one has been able to hack it, according to many organizations. As a result, Blowfish has become a popular choice among vendors and e-commerce companies, primarily for its ability to encrypt payments, passwords, and other sensitive data.

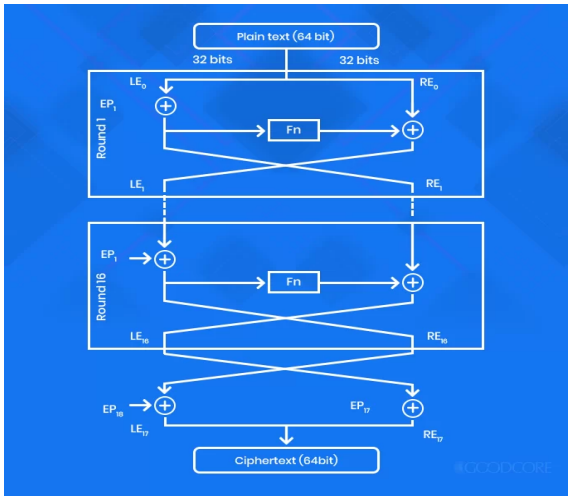

Fig. 6 Blowfish encryption model[1]

Twofish

Twofish is a more advanced form of Blowfish encryption and is also a symmetric block cipher. It has a 128-bit block size and can grow to a 256-bit key length[1]. It also divides data into fixed-length blocks, as do other symmetric ciphers. Regardless of the size of the data, it operates in 16 rounds. This method of encryption is the most adaptable of the many available. It allows you to pick between a speedy encryption process and a sluggish key setup, or vice versa. In comparison to other methods of encryption, you have complete control over this one because it is license-free and extremely fast. Twofish would have been considered one of the best encryption algorithms if AES had not been the best.

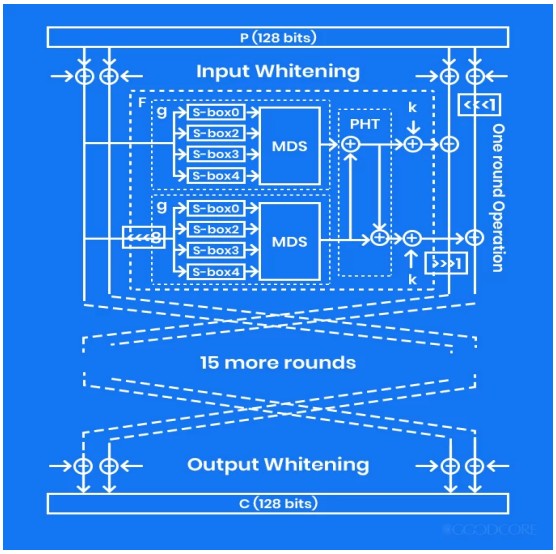

Fig. 7 Twofish encryption model[1]

VI. Encryption Algorithm Runtime

RSA, AES, Triple DES, and Blowfish have all been tested for the elapsed time when encrypting and decrypting a specified string variable. The test includes updating the string with character lengths of 15, 50, 100, 250, 500, 1,000, 5,000, and 10,000. The string used for each encryption is the same and was run ten times each to receive the average of the running time and was recorded in milliseconds. All of the data recorded was placed into a table and bar graph (used log scale for y). After recording the results, All encryptions didn't hit a significant range until it reached the one thousand to five thousand range. The RSA encryption took the longest out of the bunch, taking an average of 1324 milliseconds to encrypt and decrypt a 15 character string and 5120.5 milliseconds for a 10,000 character string. AES is next with only 409.8 milliseconds at 15 and 788.1 milliseconds at 10,000. Following AES is Blowfish which stayed in the double digits, spanning from 73.9 to 89.5 until it encrypted and decrypted a 5000 character string and jumped to an average of 231.5 milliseconds and 418.1 for 10,000. And finally, Triple DES with an average of 62 milliseconds for 15 character lengths and stayed in the low 60's to the high 70's until the string variable hit 5,000 and 10,000 where it had an average of 160.7 and 277.3 milliseconds.

Size	AES	Triple DES	RSA	BlowFish
15	409.8	62	1342	73.9
50	444.5	63.8	1258.4	68.3
100	421.2	73.4	1741.5	69.3
250	441.3	76	1741.4	71
500	451.9	76.7	1797.3	75.1
1000	456.1	78.8	1847.8	89.5
5000	618.7	160.7	3240.2	231.5
10000	788.1	277.3	5120.5	418.1

Fig. 8 Encryption Runtime data table

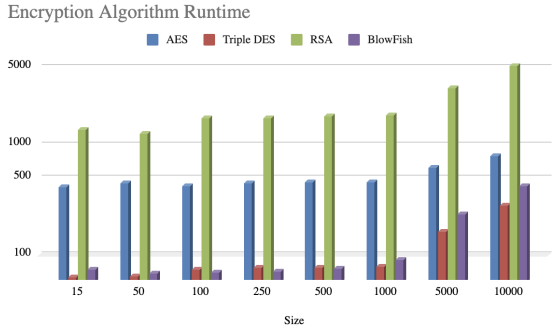

Fig. 9 Encryption Runtime bar graph

VII. Conclusion and Future Experiments

To properly conclude my investigation, I believe that AES encryption is the best of the encryptions that have been tested and described, as it is used by the United States Government to protect classified information currently. AES replaced DES and Triple DES encryption back in 2005 due to the fact that both were inefficient with brute force attacks. One of the primary objectives for the DES replacement algorithm from the National Institute of Standards and Technology (NIST) was that it be efficient in both software and hardware implementations. (Originally, DES was only practical in hardware implementations.) Performance analysis of the algorithms was carried out using Java and C reference implementations. AES was chosen in an open competition that included 15 candidates from as many research teams as possible from around the world, and the overall amount of resources dedicated to the process was enormous.

Finally, in October 2000, the National Institute of Standards and Technology (NIST) announced Rijndael as the proposed Advanced Encryption Standard (AES) [12]. RSA Encryption, however, can work together with AES. A major flaw of AES is that, as a symmetric method, it necessitates the use of the same key by both the encryptor and decryptor. This raises an essential key management issue: how can that crucial secret key be disseminated to hundreds of recipients throughout the world without incurring the danger of it being corrupted carelessly or purposefully somewhere along the way? Combining the strengths of AES and RSA encryption is the solution. The fast AES algorithm encrypts the majority of data sent in many modern communication contexts, including the internet. Authorized recipients publish a public key while keeping a private key that only they know in order to obtain the secret key needed to decrypt that material. The sender then encrypts and sends each receiver their own secret AES key, which can be used to decrypt the material, using that public key and RSA [5].

Twofish and Blowfish are both fast and compact with their own unique methods. While Blowfish uses less computing power and fewer operations to encrypt, the key schedule for the encryption is time consuming, which can be taken as a positive or a negative depending on the situation at hand. Not only that, but due to the small bits of data, probabilistic-based attacks could easily break through the algorithm. Twofish is more flexible since it gives the user full control over how fast the encryption process is as well as the combination of the best-in-class cryptography. However, the S-boxes the encryption uses makes it vulnerable to side-channel attacks.

For future research, we could try AES encryption with two keys instead of one, or discover a way to expand block lengths so that it doesn't have to rely on RSA to mask its weaknesses, and for RSA, we could try altering the algorithm so that it can handle block lengths less than a thousand. Not only that, but it would be the finest encryption of the lot if it weren't for Twofish's use of distinct keys for each data set and S-boxes. If a solution to these drawbacks can be found, it has the potential to become the most resourceful for both private and public usage.

References

1. Allan, M. (2019, October 30). *6 types of encryption that you must know about!* GoodCore Blog. Retrieved April 8, 2022, from https://www.goodcore.co.uk/blog/types-of-encryption/
2. Bendetti, G. (2022, March 22). *Quantum cryptography, explained*. QuantumXC. Retrieved April 6, 2022, from https://quantumxc.com/blog/quantum-cryptography-explained/
3. Bhat, A. (2021, September 30). *Blowfish algorithm with examples*. GeeksforGeeks. Retrieved April 8, 2022, from https://origin.geeksforgeeks.org/blowfish-algorithm-with-examples/
4. Cauz, J. (2017). *How satellites work*. Encyclopædia Britannica. Retrieved April 8, 2022, from https://www.britannica.com/technology/satellite-communication/How-satellites-work
5. Franklin, R., & Editor, P. (2021, May 13). *AES vs. RSA Encryption: What are the differences?* Precisely. Retrieved April 8, 2022, from https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences
6. Gilbort, E. (2022, January 18). *What is Data Encryption?* GeeksforGeeks. Retrieved April 8, 2022, from

https://www.geeksforgeeks.org/what-is-data-encryption/

7. Karki, D. (2020, November 9). *Can you guess how much data is generated every day?* Takeo. Retrieved April 8, 2022, from https://www.takeo.ai/can-you-guess-how-much-data-is-generated-every-day/#:~:text=With%20the%20increase%20in%20the,number%20is%20in%20increasing%20order
8. King, M., & Goguichvili , S. (2020). *Cybersecurity threats in Space: A roadmap for future policy*. Wilson Center. Retrieved April 6, 2022, from https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy
9. Knerl, L. (2019, August 21). *What are the different types of encryption?: HP® Tech takes*. What Are the Different Types of Encryption? | HP® Tech Takes. Retrieved April 8, 2022, from https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption
10. mocha, G. (2021, June 29). *Twofish vs blowfish: Encryption differences*. Gig Mocha. Retrieved April 8, 2022, from https://gigmocha.com/twofish-vs-blowfish-encryption-differences/
11. Rembert, L. (2021, August 12). *Guide to cryptography mathematics*. Privacy Canada. Retrieved April 8, 2022, from https://privacycanada.net/mathematics/
12. Security, T., & Editor, P. (2021, May 13). *AES vs. Des Encryption: Why AES has replaced DES, 3DES and TDEA*. Precisely. Retrieved April 8, 2022, from https://www.precisely.com/blog/data-security/aes-vs-des-encryption-standard-3des-tdea
13. Smith, G. (2020). *Cyber concerns for the satellite sector*. Archon Secure. Retrieved April 6, 2022, from https://www.attilasec.com/blog/satellite-cybersecurity
14. Tyagi, M. (2021, April 27). *Java program to implement the RSA algorithm*. GeeksforGeeks. Retrieved April 8, 2022, from https://www.geeksforgeeks.org/java-program-to-implement-the-rsa-algorithm/