Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Application Of Cryptography to Everyday Communication and Transactions

Apau George Sedem
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: Sedemapau22@gmail.com

ABSTRACT

Encryption and decryption techniques can be used to secure text data files on a computer. One method uses cryptography to encrypt and decrypt text files used in data encryption systems. By conducting encryption and decryption on the text file's data, cryptography is the science or art of securing and randomizing messages to prevent data manipulation. Quantum cryptography is one of the emerging topics in the field of computer industry. This paper focuses on how the Hill Cipher Text Algorithm is applied in communication specifically via text. It also further talks about modern cryptography and quantum cryptography. It explains how quantum cryptography works and how it is going to thrive in the near future.

Keywords: Cryptography, Hill Cipher, Modern Cryptography, Quantum Cryptography.

Proceedings Citation Format
Apau George Sedem (2022): Application Of Cryptography to Everyday Communication and Transactions. `Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 174-178. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P34

1. BACKGROUND OF STUDY

Today, the internet is used for all tasks relating to banking, credit cards, ATM cards, marketing, and e-commerce, among others. Thus, there must be safeguards delivered via the internet. For security, we have numerous types of cryptography for communication. We employ methods which use these cryptography techniques or strategies for handling delicate information and defend against an illegal entry. In a cryptosystem, data are secured using an encryption technique to maintain the confidentiality of communications. Everyone encrypts a private communication before sending it, and the intended recipient decrypts it using the key [1].

Perhaps the most crucial component of communication security is cryptography, which is also gaining ground as a fundamental component of computer security. The act of encoding a communication in such a way as to conceal its contents is known as encryption. A number of safe algorithms are used in modern cryptography to encrypt and decrypt messages. Each of these focuses on the use of keys, which are classified information. A cryptographic key is a component of an encryption technique that makes it impossible to decrypt data without knowing the key. The process of encoding a message in order to encrypt its contents is known as encryption.

To ensure that only the sender and the recipient can use the data, plain or regular text delivered over the network is changed into cipher text. Technically speaking, encryption is the process of transforming plain text messages into cipher text messages. Decryption is the process of turning cipher text back into ordinary text. The complete opposite of encryption is decryption. In computer-to-computer communications, encryption is typically performed at the receiving computer to transform plain text messages into cipher text messages. This message is then transmitted to the receiver over the network. The recipient's computer uses the decryption procedure to convert the encrypted communication to plain text. Cryptography is the study of encryption and decryption. In general, cryptography is the science and art of achieving protection by encrypting messages to render them illegible to read. Writing in secret is also known as cryptography, and it protects data security. Data that is well-hidden cannot be easily accessed, altered, or created [2]. Additionally, it can be used with software, graphics, or voice.

The history of encryption began during the reign of the great Julius Caesar. Caesar adopted this tactic to communicate in private. The Caesar's form, also referred to as the Caesar's Cipher, is one of the simplest encryption techniques. In comparison, modern encryption techniques are significantly more sophisticated and complex. Today, very sophisticated algorithms are used to transform understandable information into an unintelligible format [3].

Talking about the way forward, quantum computing is playing a vital role in modern day cryptography. The study of quantum computing is concerned with the creation of computer-based technologies based on the ideas of quantum theory. The nature and behavior of matter and energy at the quantum (atomic and subatomic) level are explained by quantum theory. Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked. A picture below (fig 1) shows the cryptographic process.

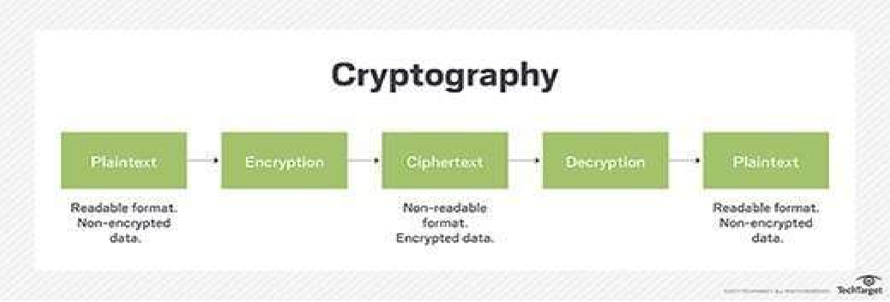
Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
TechTarget

Fig 1: The Cryptography Process
(Adapted from https://www.techtarget.com/searchsecurity/definition/cryptography)

2. REVISED LITERATURE

A computer network is a collection of computers that is intended to enable resource sharing, communication, and information access [4]. Text messaging can be classified as a popular means of communication via network. A research paper showed how to use Hill Cypher Algorithm in securing text messages. One symmetric cryptography algorithm is this one. A matrix with dimensions of m x m serves as the encryption and decryption key for the Hill Cipher algorithm. Hill Cipher's basic matrix theory involves multiplying matrices together and inverting the matrix. In general, Hill Cipher uses two different types of matrices: 2 x 2 and 3 x 3. The order 2 x 2 was discussed in that paper. It is strongly advised to employ the Hill Cipher in text-based media due of its quick encryption and decryption times. This technique is particularly effective at protecting data being transmitted over an open network [5].

Modern cryptographic methods are built on the fundamental, so-called "INTRACTABLE," process of factoring big integers into their primes. But as computing power improves and mathematics advances, one-way functions like factoring huge integers can be swiftly reversed, making current cryptography susceptible [6]. The answer was to incorporate quantum physics into cryptography, which will allow it to be evaluated. One of the newest subjects in the computer business is quantum cryptography. This study concentrated on quantum cryptography and the value that this technology adds to a defense-in-depth approach with respect to entirely secure key distribution. The development of quantum physics, or the study of how things function at the subatomic level, at the turn of the 20th century was spearheaded by a number of eminent scientists, including Schrödinger, Bohr, Heisenberg, and Einstein, among others[9]. This paper's scope included the shortcomings of contemporary digital cryptosystems, the underlying ideas behind quantum cryptography, the practical applications of this technology and its drawbacks, and ultimately the route that quantum cryptography is likely to go in the future [6]. An example of quantum cryptography is represented as an image below:

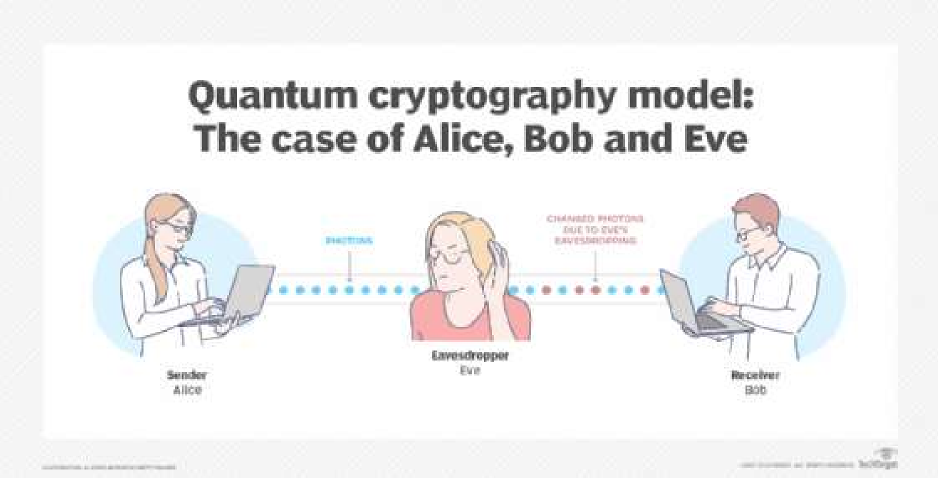

Fig 2: Quantum cryptographic model
(Adapted from https://www.techtarget.com/searchsecurity/definition/quantum-cryptography)

Lastly, another research paper looked into post quantum cryptography. All currently frequently used asymmetric cryptosystems will become insecure due to significant advances in quantum computing. The vulnerability of classical cryptosystems in the setting of quantum computing was examined in that paper, along with the various post-quantum cryptosystem families, the state of the NIST post-quantum cryptography standardization process, and a few potential future research avenues in this area [9].

3. FINDINGS

It can be shown that the cipher text created during the encryption process can be successfully converted back to plaintext without losing a single character after testing the Hill Cipher method against the plaintext "HILL CIPHERX." As a result, the Hill Cipher algorithm functions effectively when text-based messages are used [5]. The key matrix for the Hill Cipher must be an invertible matrix. The security component is stronger the larger the key matrix. While known-plaintext attacks are weak against this algorithm, cipher text-only assaults are strong against it. The key needs to be kept secret in order to protect against this algorithm. If a careless individual ends up with the key, inverse modulo can find the key through a sequence of calculations [5].

In a post-quantum future, symmetric algorithms and hash functions are comparably secure. The assaults can be accelerated by square root complexity using Grover's Algorithm [9]. The foundation of each and every asymmetric algorithm used today is a mathematical conundrum for which researchers have been looking for answers for millennia. The drawback of quantum computers is that they excel at concurrent tasks that only need one outcome in the end. A superposition of qubits can be utilized to parallelize all computations since the algorithms only need one final result, which can then be measured. Algorithms that require several results can be used to avoid utilizing quantum computers' parallelism. Quantum computers' parallelism can't be fully utilized in this way [9].

4. RESEARCH GAPS

4.1 Limitations of Modern Cryptosystems

Public key cryptography is used to exchange keys rather than encrypt large volumes of data since it requires sophisticated calculations that move slowly. To distribute symmetric keys across distant parties, for instance, widely established systems like the RSA and Diffie-Hellman key negotiation schemes are frequently utilized [6]. Given the computing capacity of today's computers, the speed of these algorithms is based on the fact that there is no known mathematical method for factoring really big integers quickly. There are a few concerns even though the public key cryptosystems in use today might be "good enough" to offer a moderately high level of confidentiality. For instance, improvements in computer processing, such quantum computing, may be able to quickly beat systems like RSA and render public key cryptosystems obsolete [6].

5. RECOMMENDATION FOR PRACTICES

Recommendation for Practices

It is recommended that the use of old encryption ciphers should not be used since they are widely known and people can decrypt them easily. Encryption keys must also be stored very well because if it falls into a wrong hand there might with issues with the integrity and confidentiality of the data encrypted.

Policies and Design

Companies must put in place the necessary technical safeguards to secure data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA). Cryptography is a technique that makes it possible to accomplish this. This covers both at rest and while in transit. It is sometimes used to maintain the integrity of data that must be precisely transferred and stored but can be viewed by anybody, anywhere.

6. CONCLUSION

Even while quantum cryptography has made significant strides over the past years, there are still obstacles to overcome before it can be used as a common key distribution system by enterprises, governments, and regular people. These difficulties specifically concern the creation of more sophisticated hardware to enable quantum key exchange at higher quality and greater transmission ranges.

7. DIRECTION FOR FUTURE WORKS

According to experts, working quantum computers will exist in ten years and will be able to perform calculations such as the prime factorization of enormous numbers millions of times quicker than conventional computers can now. Additionally, those quantum computers would be capable of breaking encryption techniques that we currently consider to be secure. Therefore efforts must be made to make this achievable in the near future as predicted.

REFERENCES

1. W. Stallings “Cryptography and network security”, vol.2, Prentice Hall, 2003
2. C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing. New Jersey: Prentice Hall, 2015.
3. Krishna A, A., & Manikandan, L. C. (2020). A Study on Cryptographic Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3307, 321–327. https://doi.org/10.32628/cseit206453
4. H. Ming dan S. LiZhong, “A New System Design of Network Invasion Forensics,” in 2009 Second International Conference on Computer and Electrical Engineering, 2009, hal. 596–599.
5. Siahaan, M. D. L., & Siahaan, A. P. U. (2018). Application of Hill Cipher Algorithm in Securing Text Messages. International Journal For Innovative Research in Multidisciplinary Field, 4(10), 55–59.
6. Dušek, M., Lütkenhaus, N., & Hendrych, M. (2006). Quantum cryptography. Progress in Optics, 49(C), 381–454. https://doi.org/10.1016/S0079-6638(06)49005-3
7. Quantum Cryptography model. Retrieved from:https://www.techtarget.com/searchsecurity/definition/quantum-cryptography.
8. Quantum Cryptography Explained. Retrieved from: https://quantumxc.com/blog/quantum-cryptography-explained/.
9. Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & Atul. (2022). Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. http://arxiv.org/abs/2202.02826