# The Era of Encryption - An Overview

**Subrata Mandal[1], Aniket Kumar Singh[2]**

[1,2]Student, Computer Science and Engineering, Lovely Professional University, India

**ABSTRACT**

**Encryption is a technique that is used to convert original information, also called plain text, into unreadable ciphertext. This is done with the help of an encryption algorithm and key. It is meant to keep the original information secured from the wrong recipient. So only the right recipient can read the information by decrypting it using the decryption algorithm and key. Throughout history, encryption has been used to transfer secret information in the military. The most famous one is Caesar cipher. This method is named after Julius Cease, it was a very basic encryption technique, and it is a substitution cipher, in which letters were replaced by shifting by a fixed number. But nowadays encryption technique has advanced.**

**Keywords: AES, DES, RSA, QKD.**

## INTRODUCTION

Cryptography is an evolving field of Computer Science, it is everywhere from a computer, smartphone, website, internet of things (IoT), etc. The modernization of technology has changed everything into digital form. Being everything digital our data and privacy are more at risk than ever and that's why we need to protect our data. This is where Cryptography and Encryption technique comes into play.

Cryptography is a study of techniques that help us secure our sensitive data at rest or data in motion. The term data at rest means it is not moving from one device to another. It is stored on a hard drive, flash drive, or web server. The data in motion means that data is moving from one location to another.

The main agenda of cryptography is to achieve four important points which are:
1) Confidentiality: it prevents unauthorized users from accessing information and ensures that only the authorized user can access the information.
2) Data integrity: It ensures the safeguard and completeness of the information. An unauthorized user cannot make modifications or alterations to data.
3) Authentication: it is a process of identifying the user by verifying their credential from the database of authorized users.
4) Non-repudiation: it means that someone cannot deny after sending a message or an email from their computer. This is accomplished by digital signature.

## VARIOUS ENCRYPTION METHODS

There are two types of cryptographic systems: Symmetric key and Asymmetric key cryptography.

**1) Symmetric Key Encryption:**
In symmetric-key cryptography, the encryption and decryption are done by the same key.it is also known as a block cipher. There are many types of symmetric key encryption techniques example: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Twofish, Serpent, and Advanced Encryption Standard (AES).

**Blowfish Encryption:**
Blowfish is a symmetric key block cipher technique designed by Bruce Schneier in 1993 and it is publically available without any patent. No license is required and the source code is available for free on the internet. When blowfish was created there was no practical attack against it. Blowfish was developed for 32-bit CPUs and has only a 64-bit block length. It can be used in the place of Data encryption standard (DES) or IDEA. It can take a variable-length key, from 32-bits to 448-bits, it was designed as a free and fast alternative to the existing algorithm. Its structure is close to that of CAST-128, which includes fixed S-boxes. The Blowfish algorithm function splits the 32-bit input into four 8-bit quarters as input to four S-boxes. The final output 32-bit is produced by adding modulo 232 and XORed. Blowfish algorithm works with derived the hexadecimal digits of pi, which has no obvious pattern.

The product uses blowfish are 96Crypt, SplashID (windows, Mac, iPhone), 1Password (Mac, iPhone), etc. But now it is not recommended by the author because of the advancement in computers.

Blowfish is a fast block cipher, but when it comes to hanging keys. It facilitates pre-processing, which is similar to handling 4 KBs of data and is very unreliable in contrast to newer encryption methods. Blowfish block cipher was vulnerable to birthday attacks. In 2016, the SWEET32 attack demonstrated how a birthday attack can recover plaintext against block cipher of 64-bit.

**Twofish Encryption:**

Twofish is an encryption algorithm that is highly secure to use. It was an advancement and up-gradation of the previous version of Blowfish.it was a team effort. Bruce Schneier was the leader of the team and they were a part of a competition held by the National Institute of Standards and Technology (NIST) for the selection of Advanced Encryption Standard (AES) in the replacement of Data Encryption Standard (DES) in the end Twofish was not selected.

Twofish is a symmetric key encryption technique, which uses the same key for encrypting and decrypting the data. It uses precomputed key-dependent S-boxes. An S-box is a basic component of any block cipher algorithm, it is also known as a substitution box. Twofish is a block cipher of size 128-bits up to 256-bits. It is fast, flexible, and secure, and it is free to use, there no licensing fee, patent on the algorithm.

There has been no successful cryptanalysis against Twofish. It is theoretically proven that any encryption technique that uses 128-bit or higher bits for encryption, is safe from brute force attack. The products that use Twofish are 96Crypt by eRightSoft, KeePass, GnuPG, PGP, etc.

**Triple-DES Encryption:**

DES is a Feistel network-based symmetric-key method. It's a symmetric key cipher, which means it uses the very same key to encrypt and decrypt. The Feistel network enables each of these mechanisms nearly identical, leading to a much more reliable method to execute. Triple DES is just an encoding method that utilizes three DES iterations on the same plain text.

It applies a variety of key selection techniques: In the first, all used keys are distinct, in the second, two keys are the same and one is separate, and in the last, all keys are just the same.

Even though 3DES is still essential in encryption as the counterpart to DES, its era has ended, so it's important to switch ahead. Since modern tech no longer trusts 3DES, its use will be phased out after 2023.

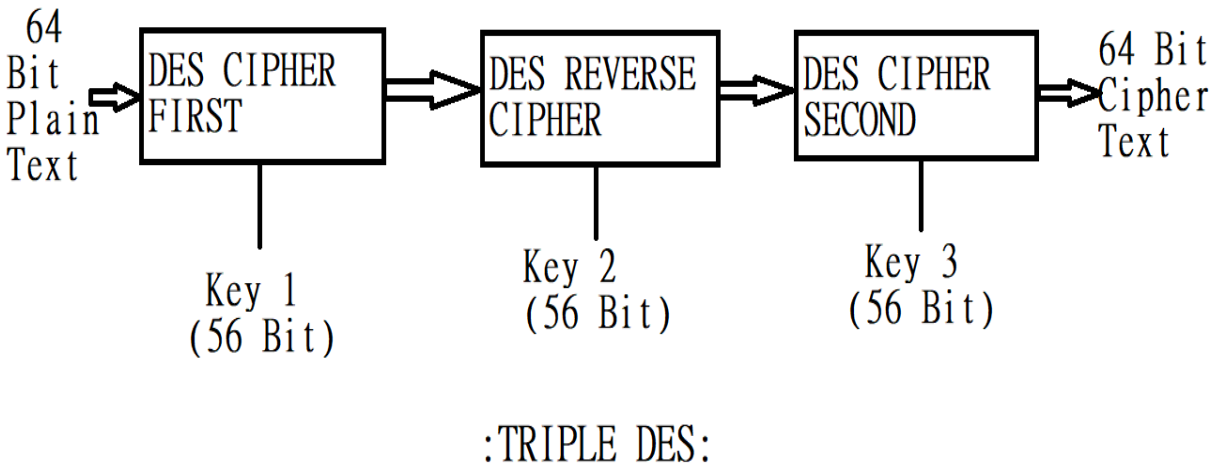


**Fig. 1:Block Diagram Of Triple DES**

**AES Algorithm in Cryptography:**

Unlike the Feistel network-based DES, AES (Advanced Encryption Standard) implements an iterative technique. AES outshines triple-DES as it is more than 6 times quicker than the triple DES. Symmetric encryption is much faster than asymmetric encryption and is frequently implemented in schemes such as database systems. AES-128, AES-192, and AES-256 are the 3 block ciphers of the Advanced Encryption Standard.

The AES symmetric encoding specifies the number of modifications to be implemented to information embedded in an array. The cipher starts by placing the information into an array, following that the cipher modifications are replicated over several encoding rounds. AES is often used for self-encrypting disc drives, network protection, and storage data security.

All of AES's computations are done on bytes instead of bits. As a result, AES considers an unencrypted block's 128 bits as 16 bytes. Those 16 bytes are structured into four columns and four rows for matrix encoding. Electronic Code Book, or ECB, is the name given to the raw AES method of operation. Since raw AES in ECB mode could leak pattern details while encrypting high amounts of information, an initialization vector is commonly used.
The Cipher Block Chaining (CBC) form of AES encryption, as well as the Counter (CTR) mode, are also frequently utilised.

Even with a 128-bit key, breaching AES by evaluating all probable key values is so computationally time consuming that even the fastest supercomputer will take more than 100 trillion years to solveit. AES has never been breached and is likely to remain secure over several years to come based on known technological trends.

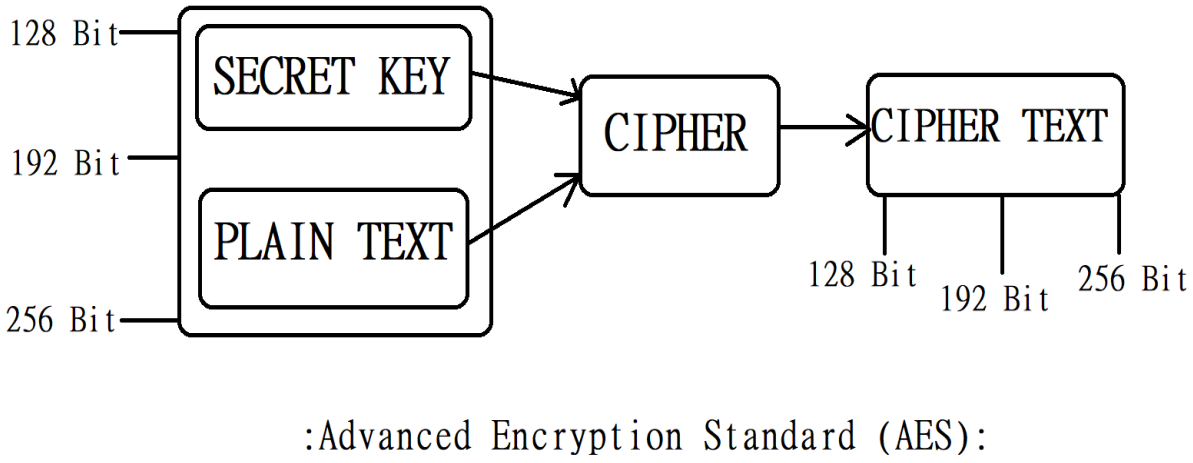


**Fig. 2: Block Diagram Of Advanced Encryption Standard**

**2) Asymmetric Key Encryption:**
Asymmetric key cryptography or mostly known as Public-key cryptography. It is a system that uses two keys which are the Public key and Privet key. A public key is openly shared and a private key is never shared. A sender can encrypt the message by the receiver's public key but that message can only be decrypted by the receiver's private key. The cryptographic algorithm which is used for generating these keys are based on a one-way mathematical function.

**RSA Algorithm in Cryptography:**
RSA (Rivest–Shamir–Adleman) cryptography is built around the belief that the technique is smooth to obtain in one way but still almost unfeasible from the opposite. For example, it is simple to verify that 113 multiplied to 337 results to 38081, but if you try to track down the chosen factors of 38081 then it is a far more complex job.

The characteristics of RSA permit public keys to be circulated without hindering the communication or uncovering the private key. RSA encoding is frequently used in association with certain other cryptographic algorithms, or even for digital certificates that justify a document's credibility as well as fairness. However, it is less accurate and resource-intensive than symmetric-key encryption, it's not popularly utilized to encode the whole documents or information.

To use RSA to encrypt the data is to build the keys. So we require two big prime numbers. The efficiency of security is directly reliant on the key length and increasing or multiplying the key length enhances the quality of protection enormously.

RSA keys are most often 1024 or 2048 bits long and to create the keys we need Euler's theorem, Euler's totient function, and modular arithmetic. Though specialists conclude that somehow the keys with 1024 bits could well be breached in the coming days by the upcoming technologies. To attain the protection of RSA with the output of AES, RSA encoding can be paired with AES symmetric cryptography.

## QUANTUM CRYPTOGRAPHY

Quantum cryptography uses the principles of quantum mechanics which depends on two properties of physics which are, Heisenberg Uncertainty principle and the polarization of the photon. Quantum cryptography was discovered by Gilles Brassard and Charles H. Bennet in 1984. The quantum properties of light can be used to send secret messages.

Quantum cryptography works on the qubit, it has the property of quantum entanglement and superposition, so it can be 0 or 1 at the same time. Photon has different polarization in wavelength. It can simply be considered as "tilt" in the light wave. There four types of polarized photon which are, vertical ( | ), horizontal ( — ), at 45 degrees ( / ) and 135degrees ( \ ). Photon states are measured by passing them through four filters vertical, right diagonal, horizontal, left diagonal or we can group them as a rectilinear filter and diagonal filter. If the polarized photon measure through the wrong filter it gets destroyed. This irreversible property of photon makes eavesdropping impossible.

**The Risk from Quantum Cryptography:**
The strongest key used in today's world has not been broken yet and it is estimated that the 2048 bit key will take millions of years to break. But the encryption method based on the large factorization method will not be safe forever because a large quantum computer will be able to run a "SHOR" algorithm. Quantum cryptography cannot crack symmetric key methods like Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), etc. But it can crack public key encryption like RSA (Rivest–Shamir–Adleman) and ECC.

National Institute of Standards and Technology (NIST) has recommended not using the 1024 bit version of RSA encryption instead of it using 2048 bit encryption. But longer keys will make encryption slower. The length of the key has to be increased substantially to stay ahead of quantum computers.

**Quantum Key Distribution (QKD):**
It is a secure way of communication that involves cryptography protocol and quantum mechanics. It enhances the public key encryption method by the unique property of quantum mechanics that can detect eavesdropping because the measuring state of quantum bits can change its property. The message which is sent to the receiver got intercepted by an eavesdropper then it would be detected.

**Post-Quantum Cryptography:**
Gilbert Vernam had invented an unbreakable encryption technique. It is called the one-time-pad or Verman cipher. The one-time-pad uses an encryption key as long as the length of massage. The key which was used before cannot be used again because it can slip some information and the key should not be shorter than the message, in this case, it could give out some information. The major drawback of this type of encryption is the difficulty of distributing the one-time key needed to encrypt the message. The Quantum key distribution (QKD) is a perfect means to distribute a one-time-pad.

## ADVANTAGES

End-to-end (E2E) encryption is immensely crucial in terms of confidentiality. End-to-end (E2E) encryption has the following perks:
1. There is no unauthorized third-party exposure.
2. It provides high data security.
3. It increases credibility.
4. It protects the privacy of a user.
5. Data stored in encrypted form.

## CONCLUSION

Over the years many encryption techniques have been found but currently, Advanced Encryption Standard (AES) is used. And it is secure and unbreakable. Quantum computing has also evolved and it has so much to offer. Quantum cryptography promises that it can solve the problem of the one-time key also known as one-time-pad distribution with the help of quantum key distribution (QKD). The most secure cryptography system security cannot make your data safe forever because humans have some weaknesses. A computer algorithm can work flawlessly but humans do not, they make mistakes. And that can sabotage everything. Some common mistakes humans make are employees writing their password on paper and leaving it on their desk, or having a very weak password, or giving out their password on a telephone to a scammer pretending to be a legitimate employee from the bank or from another source. Awareness is the solution to this problem.

## REFERENCES

[1] "Encryption - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Encryption#Modern. [Accessed: 26- Apr- 2021].

[2] "Cryptography - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Cryptography. [Accessed: 26- Apr- 2021].

[3] "Data Encryption Standard - Wikipedia", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Data_Encryption_Standard. [Accessed: 18- Apr- 2021].

[4] I. Saikumar, "DES- Data Encryption Standard", *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 3, 2017. Available: https://www.irjet.net/archives/V4/i3/IRJET-V4I3489.pdf. [Accessed 20 April 2021].

[5] D. Pandya, K. Ram, S. Thakkar, T. Madhekar and B. Thakare, "Brief History of Encryption", *International Journal of Computer Applications*, vol. 131, no. 9, pp. 28-31, 2015. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.6752&rep=rep1&type=pdf. [Accessed 17 April 2021].

[6] S. Pandey and M. Farik, "Best Symmetric Key Encryption - A Review", *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 6, no. 6, pp. 310-311, 2017. Available: https://www.researchgate.net/profile/Mohammed-Farik/publication/317913002_Best_Symmetric_Key_Encryption-A_Review/links/597a9c0d4585151e359956ff/Best-Symmetric-Key-Encryption-A-Review.pdf. [Accessed 22 April 2021].

[7] B. Schneier, "Schneier on Security: The Blowfish Encryption Algorithm", *Schneier.com*, 1993. [Online]. Available: https://www.schneier.com/academic/blowfish/. [Accessed: 22- Apr- 2021].

[8] B. Schneier, "Academic: The Twofish Encryption Algorithm - Schneier on Security", *Schneier.com*, 1997. [Online]. Available: https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html. [Accessed: 20- Apr- 2021].

[9] A. Thomas and E. Manuel, "Embedment of Montgomery Algorithm on Elliptic Curve Cryptography over RSA Public Key Cryptography", *Procedia Technology*, vol. 24, no. 6, pp. 911-917, 2016. Available: 10.1016/j.protcy.2016.05.179 [Accessed 14 April 2021].

[10] S. Heron, "Advanced Encryption Standard (AES)", *Network Security*, vol. 2009, no. 12, pp. 8-12, 2009. Available: 10.1016/s1353-4858(10)70006-4 [Accessed 18 April 2021].

[11] "IBM Cloud Docs", *Cloud.ibm.com*, 2021. [Online]. Available: https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction. [Accessed: 26- Apr- 2021].

[12] B. Aubum, "Quantum Encryption – A Means to Perfect Security?", *SANS Institute Information Security Reading Room*, vol. 1, no. 1, p. 4, 2003. Available: https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986. [Accessed 24 April 2021].