Analyzing Modern Cryptography Techniques and Reviewing their Timeline (2023)

Armaan Sidhu
3rd Year Computer Science Undergraduate
Manipal University Jaipur, Rajasthan, India

Abstract— **Cryptography has a long and fascinating history that spans thousands of years. From ancient times to the present day, people have used ciphering techniques to protect their secrets and communicate securely. This article traces the timeline of ciphering techniques in chronological order, from the earliest known examples of cryptography to the modern cryptographic systems used today. It explores the development of these techniques over time, the historical context in which they were used, and the mathematical and computational principles they rely on. By examining the evolution of ciphering techniques, we can gain a deeper understanding of how cryptography has adapted to changing technology and societal needs. This article highlights the ongoing importance of cryptography in ensuring the privacy and security of sensitive information and emphasizes the need for continued research and innovation in this critical field as well as the timeline of major events in the field of Cryptography – Particularly involving Modern Day Ciphers, which has shaped them in the form they are as of now.**

***Index Terms*— Cryptography history, Ciphering techniques, Encryption methods, Cryptanalysis, Codebreaking, Substitution ciphers, Transposition ciphers, Public-key cryptography, Cryptographic systems, Information security.**

I. INTRODUCTION

CRYPTOGRAPHY, the art of secret writing or solving codes, has been an essential part of human communication for thousands of years. From ancient times to the modern era, people have used ciphering techniques to protect their secrets and ensure secure communication. Over time, cryptography has evolved and adapted to meet the challenges of changing technology and societal needs.

The history of cryptography is a rich and fascinating subject that sheds light on the development of mathematical and computational techniques and their practical applications. In this article, we will trace the timeline of ciphering techniques in chronological order, starting with the earliest known examples of cryptography and ending with modern cryptographic systems. By examining the development of these techniques over time, we can gain a deeper understanding of how cryptography has evolved and adapted to meet the challenges of changing technology and societal needs.

The term "cipher" has its roots in the Arabic word "sifr", and it is believed that the first book on cryptology was written by the 9th century Arab Islamic scholar, al-Kindi The Greeks also developed early ciphering techniques, such as the scytale, which was used to transmit secret messages during military campaigns. The Romans used a variety of ciphering techniques, including substitution ciphers and transposition ciphers, to protect their communications. During the Renaissance, ciphering techniques became more sophisticated, with the development of the polyalphabetic Vigenère cipher.

In the modern era, cryptography has become an essential tool for ensuring secure communication over computer networks. The development of public-key cryptography in the 1970s revolutionized the field and made it possible to securely exchange information without having to first establish a secret key.

Today, cryptography plays a critical role in many aspects of our lives, from protecting online banking transactions to securing classified government communications. In addition to providing a historical perspective on the field, this article will also discuss the current state of cryptography and some of the challenges that researchers face in developing new cryptographic systems. It will highlight the ongoing importance of cryptography in ensuring the privacy and security of sensitive information and emphasize the need for continued research and innovation in this critical field.

Ciphering, also known as encryption, is the process of converting plaintext (normal human-readable message) into a coded or scrambled form known as ciphertext, using a mathematical algorithm or series of algorithms. This process is

This work was submitted to Manipal University Jaipur in regard of internal evaluation of Academics as well as submitted for publication. Author Armaan Sidhu is currently pursuing Computer Science Engineering in Third Year at Manipal University Jaipur, Jaipur, Rajasthan – 303007, India (e-mail: armaan.209301656@muj.manipal.edu).

used to ensure the confidentiality and security of the message, as only individuals with the key to decrypt the ciphertext can read the original message.

Ciphering is commonly used in computer systems and communication networks to protect sensitive information such as passwords, credit card numbers, and personal data.

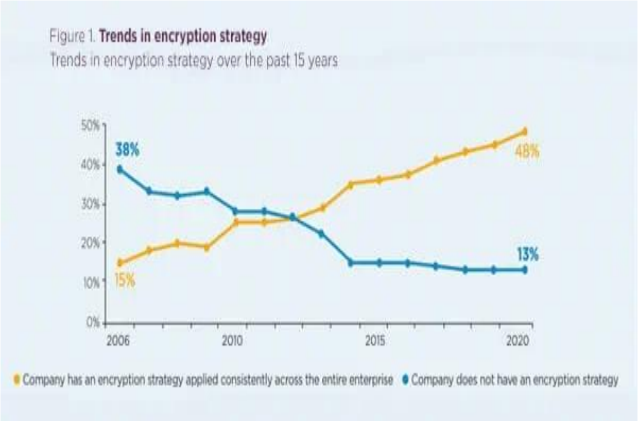


Fig. 1. *Trends in Encryption Strategy Use by Companies*. 2020 Encryption Trends Report, https://www.entrust.com/blog/2020/06/2020-encryption-trends-report/, accessed 2 March 2023.

A. Abbreviations and Acronyms

The following Abbreviations and Acronyms are used extensively in this article:

- AES: Advanced Encryption Standard
- DES: Data Encryption Standard
- RSA: Rivest–Shamir–Adleman
- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- OTP: One-Time Pad
- SSH: Secure Shell
- VPN: Virtual Private Network
- IoT: Internet of Things
- AI: Artificial Intelligence
- ML: Machine Learning
- QC: Quantum Cryptography
- PQ: Post-Quantum Cryptography
- DoS: Denial of Service
- DDoS: Distributed Denial of Service
- MITM: Man-In-The-Middle

II. RELATED WORKS

To give more prospective about the performance of the encryption algorithms, this section classifies and analysis some of the well known the cryptographic techniques for data encryption. The aspects taken into consideration for analysis are processing speed, throughput, power consumption, avalanche effect, packet size and data types.

These aspects are essential for analyzing the net overall performance of an algorithm, and these are defined as follows: -

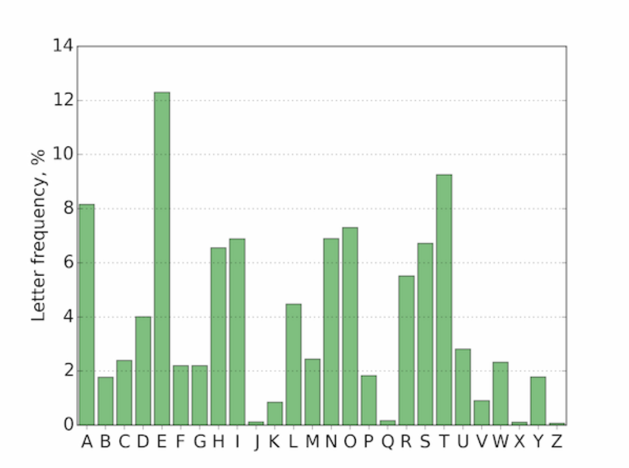


Fig. 4. *Letter Frequencies in the English language*. Scipython. https://scipython.com/book/chapter-7-matplotlib/examples/letter-frequencies-in-moby-dick/, accessed March 2nd, 2023.

- Processing speed: the rate at which a cryptographic algorithm can process data.
- Throughput: the amount of data that can be processed by a cryptographic algorithm within a given time frame.
- Power consumption: the amount of energy consumed by a cryptographic device or algorithm during operation.
- Avalanche effect: the degree to which a small change in input produces a significant change in output.
- Packet size: the size of the data blocks being transmitted or processed by a cryptographic algorithm.
- Data types: the type of data being encrypted or decrypted, such as text, images, audio, or video.

A. Classification

Ciphering techniques can be broadly classified into two categories: symmetric key cryptography and asymmetric key cryptography.

Symmetric key cryptography, also known as secret key cryptography, uses the same key for both encryption and decryption of data. This technique is generally used for encrypting large volumes of data and is faster than asymmetric key cryptography. Examples of symmetric key cryptography include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES).

Asymmetric key cryptography, also known as public key cryptography, uses two different keys for encryption and decryption of data. One key is made public and is used for encrypting data, while the other key is kept private and is used for decrypting the data. Asymmetric key cryptography is slower than symmetric key cryptography but is more secure. Examples of asymmetric key cryptography include RSA and Diffie-Hellman.

Ciphering techniques can also be further classified based on the operation performed on the plaintext, such as substitution ciphers, transposition ciphers, and modern block ciphers. Substitution ciphers involve replacing one letter or group of letters with another letter or group of letters. Transposition ciphers involve rearranging the order of the plaintext letters to form the ciphertext. Modern block ciphers involve breaking the plaintext into fixed-sized blocks and applying a mathematical function to each block to generate the ciphertext.

Substitution ciphers can be further classified into two main subtypes:

1. Monoalphabetic substitution cipher: In these, each letter in the plaintext is replaced by a fixed corresponding letter in the ciphertext. For example, in the Caesar cipher, each letter in the plaintext is shifted by a fixed number of positions down the alphabet to create the corresponding ciphertext letter.
2. Polyalphabetic substitution cipher: In these, each letter in the plaintext can be replaced by multiple different ciphertext letters, depending on its position in the plaintext. One example is the Vigenère cipher, where a series of interwoven Caesar ciphers are used with different shift values for each letter of the plaintext.

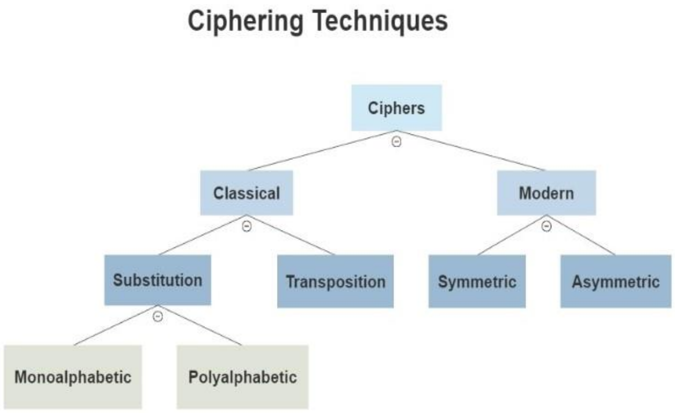


Fig. 2. *Encryption Strategy Use by Companies*. Armaan Sidhu Image Generated 2 March 2023.

B. Analysis

An analysis and comparison of the commonly used Modern Day Ciphering Techniques like DES, 3DES, AES, RSA, and Diffie-Hellman cryptographic techniques based on the chosen aspects is as follows: -

1. Processing Speed: Processing speed is an important metric to consider while evaluating cryptographic techniques as it determines the speed at which data can be encrypted or decrypted. Some of the modern cryptographic techniques that offer high processing speed include:

- AES (Advanced Encryption Standard): It is a symmetric-key encryption technique that provides fast encryption and decryption speed.
- RSA (Rivest-Shamir-Adleman): It is a public-key encryption technique that is known for its encryption and decryption speed.

2. Throughput: Throughput is the amount of data that can be transmitted per unit of time. Some of the modern cryptographic techniques that offer high throughput include:

- AES (Advanced Encryption Standard): It is a symmetric-key encryption technique that provides high throughput.
- RSA (Rivest-Shamir-Adleman): It is a public-key encryption technique that offers good throughput.

3. Power Consumption: Power consumption is an important metric to consider for cryptographic

techniques used in battery-operated devices. Some of the modern cryptographic techniques that consume less power include:

- RSA (Rivest-Shamir-Adleman): It is a public-key encryption technique that requires less power compared to other public-key encryption techniques.
- Diffie-Hellman: It is a key agreement algorithm that also requires less power compared to other cryptographic techniques.

4. Avalanche Effect: Avalanche effect is the degree to which a small change in plaintext affects the ciphertext. Mathematically it is the ratio of the number of flipped bits in ciphered text to the total number of bits in ciphered text. Some of the modern cryptographic techniques that offer a high avalanche effect include:

- AES (Advanced Encryption Standard): It is a symmetric-key encryption technique that provides a high avalanche effect.
- DES (Data Encryption Standard): It is a symmetric-key encryption technique that also offers a high avalanche effect.

5. Packet Size: Packet size is an important metric to consider for cryptographic techniques used in network communication. Some of the modern cryptographic techniques that can handle large packet sizes include:

- AES (Advanced Encryption Standard): It is a symmetric-key encryption technique that can handle large packet sizes.
- RSA (Rivest-Shamir-Adleman): It is a public-key encryption technique that can also handle large packet sizes.

6. Data Types: Different cryptographic techniques are suitable for different types of data. Some of the modern cryptographic techniques suitable for different data types include:

- AES (Advanced Encryption Standard): It is suitable for encrypting both structured and unstructured data.
- RSA (Rivest-Shamir-Adleman): It is suitable for encrypting small amounts of data and digital signatures.
- Diffie-Hellman: It is suitable for key agreement and symmetric-key encryption.

III. MODERN CIPHERING TECHNIQUES

Modern ciphering techniques are more complex and secure than traditional or classical encryption techniques. They use mathematical algorithms and keys to transform plaintext into ciphertext, making it much harder for unauthorized individuals to access or read the original message.

Modern ciphers can be broadly categorized into two main categories: symmetric key ciphers and asymmetric key ciphers.

Symmetric key ciphers, also known as shared secret ciphers, use the same key for both encryption and decryption. The most popular symmetric key cipher is the Advanced Encryption Standard (AES). Other popular symmetric key ciphers include DES, 3DES.

Asymmetric key ciphers, also known as public key ciphers, use two different keys: a public key for encryption and a private key for decryption. The most popular asymmetric key cipher is the RSA algorithm. Diffie-Hellman Key Exchange is another popular asymmetric key cipher.

Both symmetric key ciphers and asymmetric key ciphers have their own advantages and disadvantages. Symmetric key ciphers are generally faster and more efficient than asymmetric key ciphers, but they require the secure distribution of the key. Asymmetric key ciphers, on the other hand, are slower and less efficient but do not require a secure distribution of keys, making them suitable for applications like digital signatures and key exchange.

The Following Modern Ciphering techniques are examined in detail in this section: -

A. Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric key block cipher that was developed in the early 1970s by IBM, and later adopted by the National Bureau of Standards (NBS) in the United States as a federal standard for encryption. DES has since been replaced by more modern ciphers, such as the Advanced Encryption Standard (AES), but it remains an important part of the history of modern cryptography.

DES operates on fixed-length blocks of 64 bits and uses a 56-bit key to encrypt and decrypt data. The encryption process involves multiple rounds of substitution and permutation, which transform the plaintext block into the ciphertext block. The key is used to generate a series of subkeys that are used in each round of the encryption process.

The key length of DES is considered too short by modern standards, as it can be broken with a brute-force attack using modern computing power. However, there are various modifications and extensions to the original DES algorithm that have been developed to increase its security. Triple DES (3DES) is one such modification, which applies the DES algorithm three times with different keys, effectively increasing the key length to 168 bits.

DES is still used in some legacy systems, but it has largely been replaced by more modern and secure ciphers, such as AES. Despite its shortcomings, DES remains an important milestone in the history of cryptography and paved the way for the development of modern cryptographic techniques.

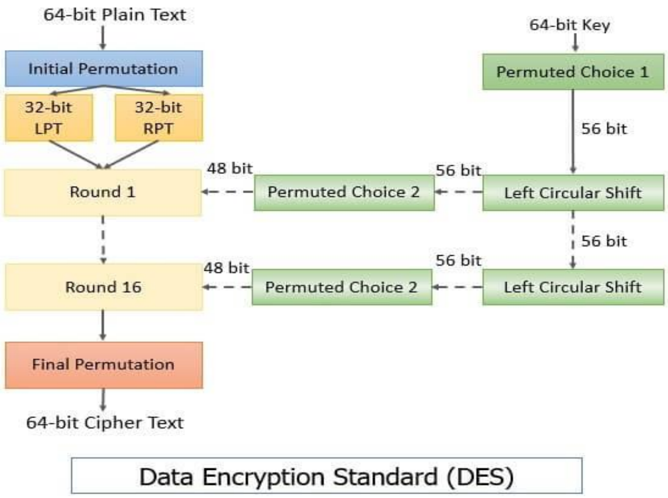


Fig. 3. *Data Encryption Standard*. BinaryTerms, https://binaryterms.com/data-encryption-standard-des.html, accessed on March 2nd, 2023.

B. Triple DES (3DES)

Triple DES (3DES) is a symmetric key block cipher that is a modification of the original Data Encryption Standard (DES) cipher. 3DES is often used in legacy systems that require strong encryption but cannot upgrade to a more modern cipher like the Advanced Encryption Standard (AES).

3DES applies the DES cipher three times to each block of data, using two or three different keys. The keys can either be independent, or the same key can be used for two or all three of the encryptions. This process is called "keying options."

3DES operates on 64-bit blocks of data, just like the original DES. However, the key length for 3DES is 168 bits, making it significantly more secure than DES. Because 3DES applies the DES cipher three times, it is more secure than a single DES encryption.

One potential drawback of 3DES is its relative slowness compared to modern ciphers like AES. However, 3DES is still widely used in legacy systems and is a reliable and secure cipher for many applications. In addition, it is compatible with existing DES implementations and requires no significant hardware upgrades to implement.

Overall, 3DES is a reliable and secure cipher that has stood the test of time. However, it is recommended that organizations that require strong encryption should consider upgrading to a more modern cipher like AES if possible.

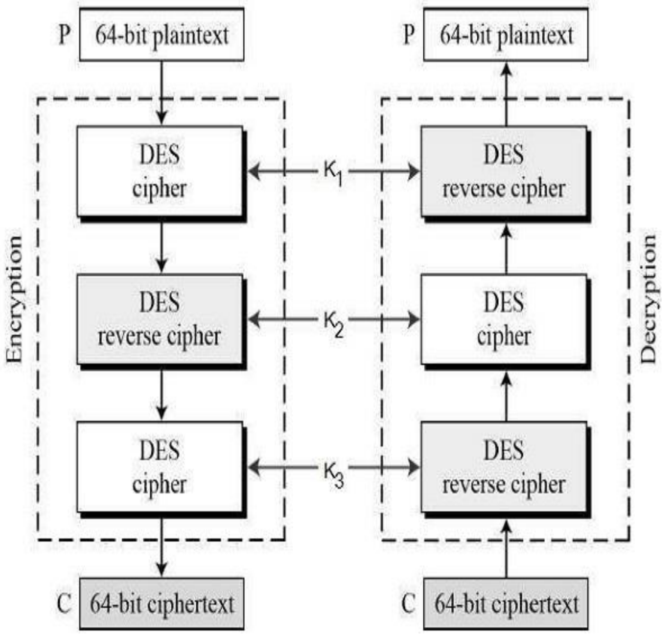


Fig. 4. *Triple Data Encryption Standard*. Tutorials Point, https://www.tutorialspoint.com/cryptography/triple_des.html , accessed March 2nd, 2023.

C. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric key block cipher that is widely used for data encryption. It was developed in the late 1990s as a replacement for the aging Data Encryption Standard (DES) cipher, which had become vulnerable to brute-force attacks due to its relatively short key length.

AES operates on fixed-length blocks of 128 bits and uses a key size of 128, 192, or 256 bits. It employs a series of substitution and permutation operations to transform the plaintext block into the ciphertext block. AES uses a "key schedule" algorithm to generate a series of round keys that are used in each round of the encryption process.

The AES system follows a specific process for encrypting and decrypting data. The number of rounds it goes through depends on the size of the key used. For 128-bit keys, there are 10 rounds, for 192-bit keys there are 12 rounds, and for 256-bit keys, there are 14 rounds. The result is either the final cipher-text or the original plaintext. AES can handle a 128-bit data length, which is divided into four basic operational blocks. These blocks are arranged in a matrix of 4x4 order and are treated as an array of bytes known as the state. The encryption and decryption processes both start with an AddRoundKey stage.

Before it reaches the final round, the output undergoes nine primary rounds, each of which consists of four transformations: Sub-bytes, Shiftrows, Mix-columns, and Add round Key. These transformations are performed during each of the nine rounds, in the tenth and final round, there is no Mix-column transformation.

The AES encryption algorithm is composed of four distinct transformations that govern each round of encryption. The first transformation is called Substitute Byte and involves converting each 8-bit byte of a 128-bit data block into a new block using an 8-bit substitution box known as Rijndael Box. The second transformation is Shift Rows, which rearranges the bytes in the last three rows of the state depending on their row location. The third transformation is Mixcolumns, which involves multiplying each column of the state by a fixed matrix. Finally, the fourth transformation is Addroundkey, which XORs the 128 bits of the present state with the 128 bits of the round key. This transformation is reversible and serves as its own inverse.

One of the key advantages of AES over DES is its significantly longer key length, which makes it much more difficult to crack using brute-force attacks. In addition, AES is faster and more efficient than DES, making it suitable for a wide range of applications, from securing data on hard drives to encrypting internet traffic.

AES has been adopted by a wide range of organizations and is used in many different applications, including in government and military contexts. It is also used by many web browsers to secure HTTPS connections.

One potential weakness of AES is that it can be vulnerable to side-channel attacks, which exploit vulnerabilities in the physical implementation of the cipher. However, this is a relatively uncommon attack vector and can be mitigated through careful design and implementation.

Overall, AES is a highly secure and efficient cipher that has become the standard for data encryption in many different applications. Its long key length and efficient design make it a reliable choice for securing sensitive data in a wide range of contexts.

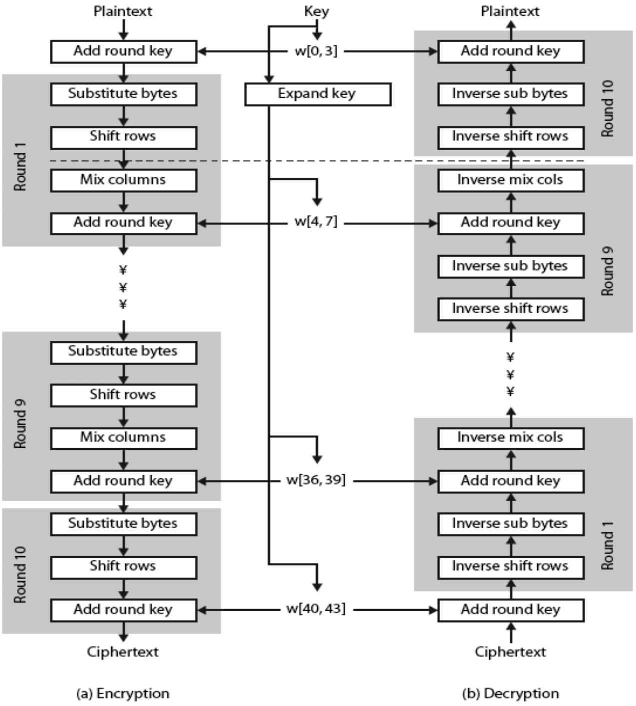


Fig. 4. *Mohammad Abdullah. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. ResearchGate. https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data, accessed 2nd March 2023*

D. Rivest-Shamir-Adleman (RSA)

RSA is a public key encryption algorithm that was first introduced by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. RSA is named after the surnames of the three inventors. It is widely used for secure data transmission and is an important part of modern cryptography.

RSA encryption is based on the mathematical concept of prime numbers. The algorithm uses a public key and a private key. The public key can be shared with anyone, while the private key is kept secret. The public key is used to encrypt data, while the private key is used to decrypt data.

The security of RSA is based on the difficulty of factoring large prime numbers. To generate a pair of RSA keys, two large prime numbers are selected and multiplied together to create a large composite number. This composite number is used as the modulus for the RSA keys. The factors of the modulus are kept secret, forming the private key, while the modulus itself is used as the public key.

RSA is widely used in secure communication protocols such as Secure Socket Layer (SSL) and Transport Layer Security

(TLS) for secure web browsing, secure email, and secure file transfers. It is also used for digital signatures, where the signer's private key is used to create the signature, and the recipient's public key is used to verify the signature.

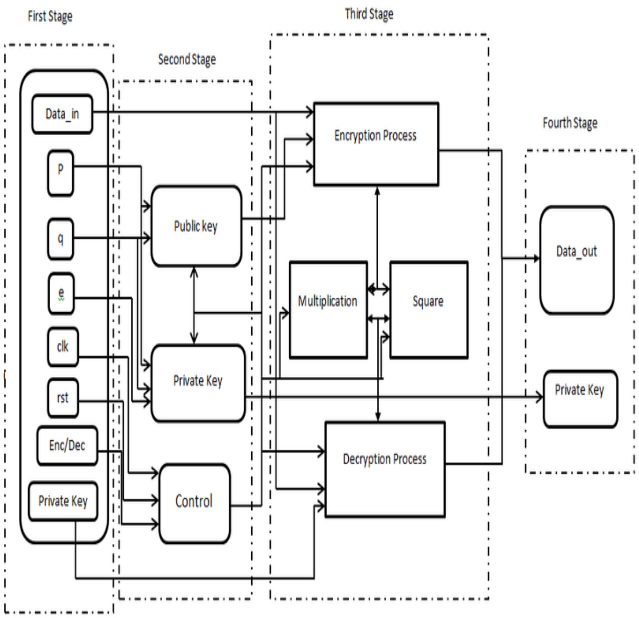


Fig. 4. Shawkat Tahir (2015) *RSA Algorithm*. ResearchGate, https://www.researchgate.net/publication/282249995_Design_and_Implementation_of_RSA_Algorithm_using_FPGA, accessed March 2nd, 2023.

The following is a procedure for key generation, encryption, and decryption:

Procedure for Key Generation

1. Select two different prime numbers p and q, both of which are large and random, and make sure p is not equal to q.
2. Compute the value of n by multiplying p and q together.
3. Calculate phi(n) by using the formula phi(n) = (p-1)(q-1).
4. Pick an integer e such that 1<e<phi(n).
5. Calculate d to satisfy the equation d × e = 1 mod phi(n); keep d as the private key exponent.
6. The public key is (n, e), and the private key is (n, d). It is important to keep d, p, q, and phi secret.

Encryption

Plaintext: P < n
Ciphertext: C = (P to the power of e) mod n

Decryption

Ciphertext: C
Plaintext: P = (C to the power of d) mod n

One potential weakness of RSA is its vulnerability to attacks based on quantum computing. Quantum computers could potentially break RSA encryption by efficiently factoring the modulus into its prime factors, rendering RSA insecure. However, this is still a theoretical concern, as quantum computers have not yet reached the necessary level of maturity to break RSA encryption.

Overall, RSA is a highly secure and widely used public key encryption algorithm that has become an important part of modern cryptography. Its reliance on the difficulty of factoring large prime numbers makes it a reliable choice for secure communication and digital signatures.

E. Diffie-Hellman Key Exchange (DHKE)

DHKE is a cryptographic protocol used to establish a shared secret between two parties over an insecure channel. It was invented by Whitfield Diffie and Martin Hellman in 1976 and is widely used in internet security protocols.

DHKE allows two parties, typically named Alice and Bob, to agree on a shared secret that can be used to encrypt their communication. The protocol works by taking advantage of the mathematical properties of prime numbers and modular arithmetic. Alice and Bob both agree on a large prime number and a primitive root modulo of that number.

Alice and Bob then each choose a secret number and perform a series of modular exponentiations to generate a public key. They exchange these public keys, which allows each party to calculate the shared secret using their own secret number and the other party's public key. The shared secret can then be used as a key for symmetric encryption, which is more efficient than public-key encryption for encrypting large amounts of data.

DHKE is widely used in internet security protocols such as Transport Layer Security (TLS), which is used to secure HTTPS connections. DHKE is particularly useful for secure communication over the internet, as it allows two parties to establish a shared secret even if an attacker is listening in on their communication.

One potential weakness of DHKE is the possibility of a man-in-the-middle attack, where an attacker intercepts and alters the public keys exchanged by Alice and Bob. To mitigate this risk, DHKE is typically used in combination with other cryptographic protocols, such as digital signatures, to verify the authenticity of the public keys.

Overall, DHKE is a widely used and important cryptographic protocol that allows two parties to establish a shared secret over an insecure channel. Its use of modular arithmetic and prime numbers make it a reliable and efficient method for establishing secure communication.

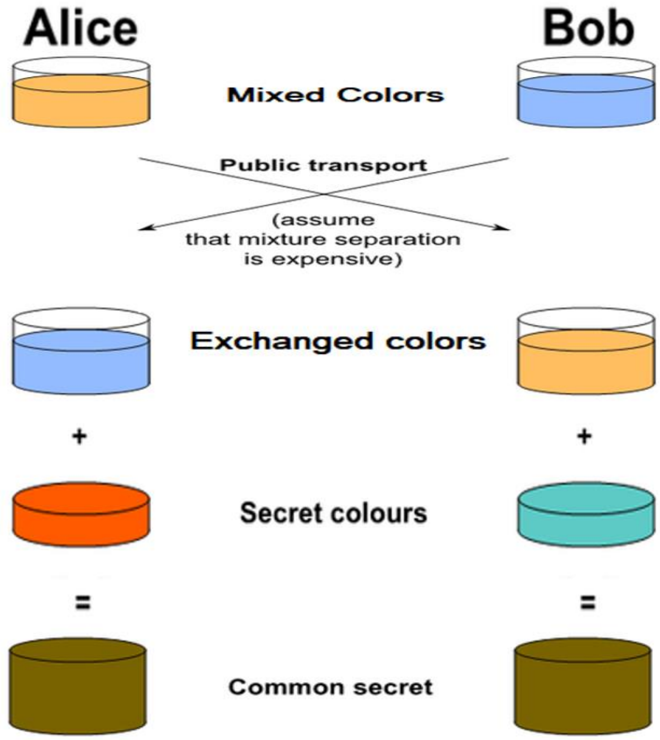


Fig. 4. *Diffie-Hellman Key Exchange*. https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange/, accessed March 2nd, 2023.

IV. TIMELINE OF MODERN CIPHERS

Cryptography, the art of securing communication, has a rich and complex history that spans thousands of years. From ancient ciphers to modern encryption methods, cryptography has evolved and adapted to meet the challenges of an ever-changing world. This section will explore the timeline and major historical events in the history of modern ciphering techniques.

- Early 20th century: One of the earliest modern ciphering techniques is the rotor machine, which was invented by Arthur Scherbius in 1918. The rotor machine used a series of rotating disks, or rotors, to encode and decode messages. Each rotor had a set of contacts that corresponded to different letters in the alphabet, and the position of the rotors determined the encryption key. The rotor machine was used by the German military during World War II to encrypt their communications.

- 1940s: During World War II, codebreaking played a crucial role in the outcome of the war. The Allies relied on several techniques, including the use of early computers such as the Colossus machine to decrypt encrypted messages. The German Enigma machine, which used rotor technology, was eventually cracked by the Allies, leading to a significant advantage in the war effort.

- 1970s: In the early 1970s, IBM developed the Data Encryption Standard (DES) as a symmetric key encryption method. DES became the standard encryption algorithm for the US government, and it was widely adopted by the private sector. However, DES was later found to be vulnerable to brute force attacks, and its key length of 56 bits was considered too short to provide adequate security.

- In 1975, Whitfield Diffie and Martin Hellman, both researchers at Stanford University, published a paper titled "New Directions in Cryptography". In this paper, they proposed a new method of cryptography that used public keys and private keys. This method, which came to be known as public-key cryptography, allowed two parties to communicate securely over an insecure channel without ever having to exchange their secret key.

- 1980s: In 1985, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, which is a public-key encryption method. RSA uses two keys, a public key and a private key, to encrypt and decrypt data. RSA is widely used today for secure communication over the internet, including email encryption, secure web browsing, and secure online transactions.

- 1990s: In the late 1990s, the Advanced Encryption Standard (AES) was developed as a replacement for DES. AES is a symmetric encryption method that uses block ciphers, which means that it encrypts data in fixed-size blocks. AES uses keys that are 128, 192, or 256 bits in length, making it much more secure than DES. AES is widely used today in various applications, including cloud computing, mobile devices, and online transactions.

- 2000s: In 2005, the US government announced that it would no longer use DES as its standard encryption algorithm and recommended the use of AES instead. In 2007, the National Institute of Standards and Technology (NIST) issued a recommendation to use the Triple Data Encryption Standard (3DES) as a replacement for DES.

- 2010s: In 2013, Edward Snowden, a former NSA contractor, leaked classified documents revealing the extent of US government surveillance programs. The leaks led to increased public scrutiny of encryption and privacy, as well as renewed interest in developing new encryption methods.

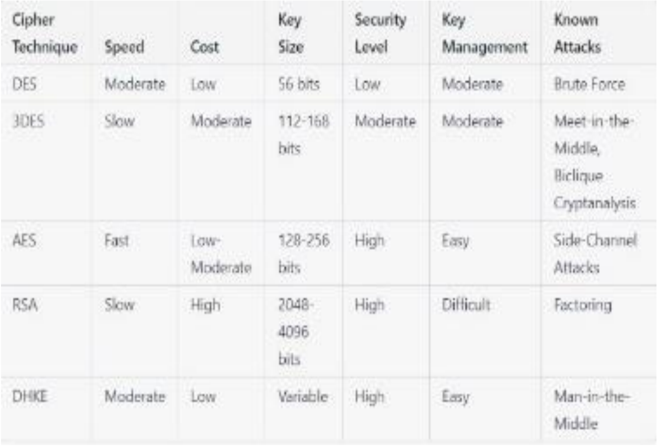
- Today: Modern ciphering techniques continue to evolve, with ongoing research in areas such as quantum cryptography, post-quantum cryptography, and homomorphic encryption. These new encryption methods are designed to provide even greater security and privacy in an increasingly digital world.

To Conclude the timeline, the history of modern ciphering techniques is a fascinating and complex story that spans more than a century. From the rotor machines used by the German military during World War II to the advanced encryption methods used today, cryptography has played a crucial role in shaping the modern world. As technology continues to evolve, it is likely that new encryption methods will be developed to meet the challenges of an increasingly connected and digital world.

V. COMPARITIVE STUDY OF CIPHERS

This section deals with the concise and precise comparative study of all the Ciphering Techniques used in the Modern day discussed so far.

TABLE I
Comparison of Modern Ciphers



Cipher Technique	Speed	Cost	Key Size	Security Level	Key Management	Known Attacks
DES	Moderate	Low	56 bits	Low	Moderate	Brute Force
3DES	Slow	Moderate	112-168 bits	Moderate	Moderate	Meet-in-the-Middle, Biclique Cryptanalysis
AES	Fast	Low-Moderate	128-256 bits	High	Easy	Side-Channel Attacks
RSA	Slow	High	2048-4096 bits	High	Difficult	Factoring
DHKE	Moderate	Low	Variable	High	Easy	Man-in-the-Middle

Notes on the table:

- Speed: Refers to the speed of encryption and decryption, with Fast being the fastest and Slow being the slowest.
- Cost: Refers to the cost of implementation, with Low being the lowest and High being the highest.
- Key Size: Refers to the size of the key used for encryption and decryption, where Variable means that the key size can be adjusted.
- Security Level: Refers to the strength of the cipher against attacks, with Low being the weakest and High being the strongest.
- Key Management: Refers to the difficulty of managing the keys, with Easy being the easiest and Difficult being the hardest.
- Known Attacks: Refers to the known attacks against the cipher, which can be used to break it.

However, the parameters for each cipher technique may vary based on implementation and usage. And the choice of cipher technique depends on the specific needs and requirements of the application or system being secured.

VI. CONCLUSION

In conclusion, modern cryptography techniques have come a long way since the days of simple substitution ciphers and have evolved to be more secure, efficient, and versatile. The timeline of cryptography shows that the development of cryptography techniques has been heavily influenced by military and political needs, as well as advancements in technology and mathematics.

Today, we have a wide range of cryptographic techniques available, including symmetric ciphers like DES, 3DES, and AES, asymmetric ciphers like RSA, and key exchange protocols like DHKE. Each technique has its strengths and weaknesses, and choosing the right technique depends on the specific use case and threat model.

While modern cryptography techniques provide strong protection against many types of attacks, they are not immune to all attacks, and new attacks and vulnerabilities are constantly being discovered. It is important for cryptographers and security professionals to stay up to date with the latest developments in cryptography research and to apply best practices in implementation and usage to ensure the security of our digital world.

Overall, the study of cryptography remains an important field of research and development, and the evolution of cryptography techniques is likely to continue as the digital landscape and threat models evolve.

APPENDIX

Glossary

- Block Cipher: A symmetric encryption algorithm that encrypts data in fixed-size blocks.
- Cipher: An algorithm used for encryption or decryption.

- Cryptanalysis: The study of analyzing cryptographic systems with the goal of breaking them.
- Cryptography: The study of secure communication in the presence of third parties.
- Decryption: The process of converting encrypted data back into its original plaintext form.
- Encryption: The process of converting plaintext into ciphertext using a cipher or algorithm.
- Hash Function: A mathematical function that converts an input message into a fixed-size output known as a hash value.
- Key: A secret value used by a cryptographic algorithm to encrypt and decrypt data.
- Key Exchange: The process of securely exchanging keys between two parties over an insecure channel.
- Key Management: The process of generating, distributing, storing, and revoking cryptographic keys.
- Plaintext: The original, unencrypted message.
- Public Key Cryptography: A cryptographic system that uses a pair of keys, one for encryption and one for decryption, with the encryption key being publicly available.
- Secret Key Cryptography: A cryptographic system that uses a single secret key for both encryption and decryption.
- Symmetric Encryption: A form of encryption that uses the same key for both encryption and decryption.
- Asymmetric Encryption: A form of encryption that uses a pair of keys, one for encryption and one for decryption.
- Digital Signature: A mathematical scheme used to verify the authenticity of digital documents or messages.
- Certificate Authority: A trusted entity that issues digital certificates used to verify the identity of users, devices, or organizations.

REFERENCES AND FOOTNOTES

A. References

- Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
- National Institute of Standards and Technology (NIST). (2001). FIPS 197: Advanced Encryption Standard (AES). U.S. Department of Commerce.
- National Institute of Standards and Technology (NIST). (2015). FIPS 180-4: Secure Hash Standard (SHS). U.S. Department of Commerce.
- National Institute of Standards and Technology (NIST). (2018). SP 800-57 Part 1: Recommendation for Key Management. U.S. Department of Commerce.
- National Institute of Standards and Technology (NIST). (2022). SP 800-56C Rev. 1: Recommendation for Key Derivation through Extraction-then-Expansion. U.S. Department of Commerce.
- Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120–126.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.

B. Footnotes

1. "Perfect secrecy" means that the ciphertext provides no information about the plaintext, even if the adversary has unlimited computational power and time.

2. In practice, many symmetric ciphers use a mode of operation such as CBC, CFB, or OFB to add randomness and diffusion to the plaintext before encryption.

3. The birthday problem states that if there are n people in a room, the probability that at least two of them have the same birthday is about 50% when n is around 23. This concept applies to hashing because the hash function maps an arbitrarily large input space into a fixed-size output space, which can lead to collisions (i.e., different inputs mapping to the same output) if the output space is not sufficiently large.

4. The term "crypto wars" refers to the political and legal debates in the 1990s over the use of strong encryption, which were triggered by concerns of law enforcement and national security agencies that criminals and terrorists would use encryption to hide their activities from surveillance and investigation. The debates involved issues such as export controls, key escrow, and backdoor access to encrypted communications.

5. A "side-channel attack" refers to an attack that exploits information leaked by a cryptographic implementation, such as timing, power consumption, electromagnetic radiation, or sound, rather than directly attacking the cryptographic algorithm or key. Side-channel attacks can be very effective against

hardware or software that does not properly protect against them.

6. An "oracle" is an imaginary black box that can answer queries about a cryptographic system, such as encrypting or decrypting messages, without revealing any internal secrets or keys. Oracles are often used in cryptanalysis to test the security of a system under different scenarios.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have contributed to the completion of this technical article.

First and foremost, I would like to thank my colleagues and mentors for their guidance, insights, and feedback throughout the research and writing process. Their expertise and support have been invaluable in shaping the content and improving the quality of the article.

I would also like to thank the academic and research communities for their continuous efforts in advancing the field of cryptography, and for sharing their knowledge and findings through publications, conferences, and online resources.

Finally, I would like to acknowledge the inspiration and motivation provided by the digital world and its ongoing evolution, which underscores the need for continued research and development in cryptography to protect our information and privacy.

Once again, thank you to everyone who have contributed to this article in any way, shape, or form.

Armaan Sidhu born 11th October 2003 in Gwalior, Madhya Pradesh, India is an Undergraduate Engineering Student currently pursuing *computer science with cyber security as program elective* in Penultimate Year at Manipal University Jaipur, Rajasthan.

He has gained a great amount of experience by working upon several tasks in Internships, with work experience including (but not limited to):

- Web Development remote internship, started January 2023, at WictroniX, a startup providing B2B IT Services and Consultations to Established Companies, launched in Late 2022 and registered by the Government of India

- Content Writing remote internship, June 2021 – March 2022 at smartwords.in, an online blogging website.

The Author is the first Vice President and one of the founding members of Eco-Tech Empire, a club established in Manipal University Jaipur which incorporates the principles of Green Computing, Cyber Security and Research Work.