JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Analysis Of Various Encryption & Decryption Algorithms Used In Cloud Computing

**Bhupender**

M.Tech. Scholar, Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana (India)

**Ms. Neha**

Assistant Professor, Department of CSE, BRCM CET, MDU Rohtak, Haryana (India)

**ABSTRACT**

"Cloud Computing is a swiftly advancing technology field, leading to a new epoch where on-demand network access to a pool of scalable computing resources is the norm. This document delivers a thorough exploration of cloud computing, discussing its assorted service & deployment models, its advantages & its pivotal role in current businesses. The study also delves into the crucial matter of cloud security, a major issue considering the increasing reliance on cloud-based solutions. As data transmission, storage & processing within cloud computing are facilitated over the internet, numerous security threats, susceptibilities & risks arise that must be identified, evaluated & reduced.[1] This paper meticulously examines key security issues such as data breaches, insider threats, account takeovers & harmful attacks & the countermeasures & mechanisms, including encryption, identity & access control, intrusion detection systems & security protocols, used to alleviate these risks. This study strives to provide a deep comprehension of the interrelationship between cloud computing & its security elements, underscoring the necessity of employing secure cloud computing in our increasingly digital world".[2]

**Keywords:-** Cloud Computing, Cloud Security, Encryption & Decryption Algorithms, Cryptography, AI & ML.

## 1. Introduction:-

The realm of encryption & decryption methodologies is primarily divided into two major types: Symmetric key & Asymmetric key cryptography. Each category encompasses numerous algorithms that carry out the encryption & decryption processes.

a) Symmetric Key Cryptography: In this paradigm, a single key serves the dual purpose of both encrypting & decrypting data. Both the sender & receiver utilize this shared secret key. Here are several of the prevalent symmetric key algorithms:

- "Advanced Encryption Standard (AES): Recognized for its robust security & efficiency, AES is a widely employed symmetric encryption algorithm. It can operate with key sizes of 128, 192 & 256 bits.

➢ Varieties of AES: Contrary to DES, AES doesn't possess multiple versions. Nonetheless, it supports various key lengths, effectively serving as different types:

- AES-128: Utilizes a 128-bit key. This type is the most resource-efficient form of AES, although it offers the lowest security level (still highly secure for practical purposes).
- AES-192: Employs a 192-bit key size, providing a balanced compromise between performance & security.
- AES-256: The most secure form of AES leverages a 256-bit key size. This version is typically used in situations where the security of data is paramount, but it demands the highest computational resources.
- Data Encryption Standard (DES): Is was truly one of the foremost well known symmetric key calculations, but its helplessness to brute-force assaults has driven to its substitution by more secure procedures.

➢ Varieties of DES:

- Single DES (S-DES): This is the fundamental version of DES that employs a singular 56-bit key for executing both encryption & decryption operations.
- Triple DES (3DES): Developed as a response to the vulnerabilities of Single DES, Triple DES uses the DES algorithm thrice on every block of data. It employs either two keys (with an overall key length of 112 bits) or three keys (resulting in a 168-bit key length). 3DES offers considerably better security than Single DES, though at the cost of a higher computational load.

- Blowfish & Twofish: Blowfish is revered for its speed & efficacy. Its successor, Twofish, offers robust flexibility & is available free of charge for public use."[45]

b) Asymmetric Key Cryptography: Moreover alluded to as open key cryptography, this approach utilizes particular keys for the encryption & decoding forms. A open key is utilized for encryption, whereas a private key is utilized for decoding. The taking after are a few of the commonly utilized deviated key calculations:

- "RSA (Rivest-Shamir-Adleman)[40]: It is among the first public-key cryptographic systems, is widely used for the transmission of safe data. The way it operates relies on the complicated computation of finding the factors of two extremely large prime numbers"
- Diffie-Hellman: Basically this algorithm enables the safe sharing of confidential keys through an unsecured network.
- Elliptic Bend Cryptography (ECC): Basically a variation of open key cryptography, is built upon elliptic bends. It offers comparable cryptographic quality as other strategies but with shorter keys, upgrading its productivity.
- Digital Signature Algorithm (DSA): DSA's primary usage lies in the creation of digital signatures for authenticating electronic documents.

## 2. Algorithms in detailed

Cloud computing allows customers to store information on inaccessible servers that they do not claim. These cloud administrations are provided by CPs (cloud providers). CP seems to have hit information security issues, so customers can't get information clarity incident data. The framework must maintain the encrypted information so that the client has access to the first information, so to speak. This is usually done using some encryption & decryption calculations. The Progressed Encryption Standard (AES) is used to ensure information evaluation. Create a digital signature verified using Advanced Flag Calculation (DSA). So the client has the right to change the information, so to speak & the changes are re-encrypted.
Encryption is critical to information security & can provide information security for enforcement, audit & acquisition systems. It is performed using symmetric & inverse calculations. Essential symmetric computations include DES, AES & 3DES.[13]

**1) DES (Data Encryption Standard):** Information Encryption Standard (DES) is an symmetric used key calculation that is used to encrypt the advanced information. In spite of the fact that it's presently considered to be 'broken', DES played a vital part within the improvement & popularization of present day cryptography. DES was developed by IBM in the 1970s & obtained by the US government in 1977. as the Official Government Data Processing Standard (FIPS) for unclassified use. The coding calculation was then freely downloaded.

Here's a fundamental outline of how DES works:

- "Key era: DES uses a 64-bit key, but 8 bits are used to check parity that result a key [36] in the length of 56 bits. This key can be used for encryption & decryption"
- Introductory stage: Information to be scrambled is orchestrated in a specific arrange. It's an cluster of 64 bits.

A. **Round function**: The data goes through 16 rounds of the same function. Each round involves the following steps:

- Extension: The information is extended from 32 bits to 48 bits.

**1)** Key blending: The extended information is combined with a circular key (inferred from the first key) utilizing the XOR operation.

**2)** Substitution: The information is passed through 8 S-boxes (substitution boxes), each of which acknowledges 6 bits of input & produces 4 bits of yield.

**3)** Change: The 32 bits from the S-boxes are improved.

**4)** Swapping: The yield of the circular work is swapped for the another circular.[5]

B. Final permutation: After the 16 rounds, the final block is rearranged once again.

The unscrambling handle employments the same steps but in invert arrange, beginning with the ultimate stage, at that point going through the rounds in invert & wrapping up with the introductory change.

The DES was considered to be secure for a long time until specialized equipment & strategies were created to abuse its moderately brief key length (56 bits). This driven to the improvement of Triple DES (3DES), This involves repeating the DES computation thrice for every piece of information. Subsequently, AES was developed to replace DES & is now the prevailing standard.

The method of DES is appeared in Figure 1 here underneath:

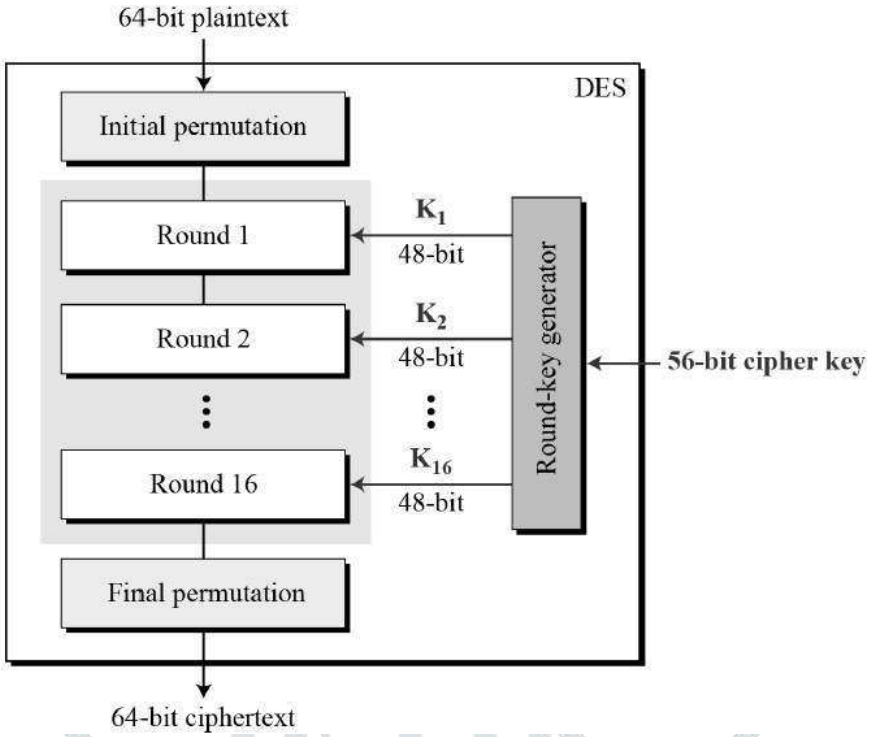


Figure 1:- Data Encryption Standard

**2) RC6 (Rivest Cipher):-** The RC6 cipher may have been based on the symmetric RC5 cipher, which operates using a square pattern. The finalists of the RSA Security Progressed Encryption Standard (AES) competition included Ronald Rivest, Matt Robshaw, [40] Ray Sidney & Yiqun Lisa Yin, who were the creators of the technology.. The "RC" in its title stands [40] for "Rivest Cipher" or "Ron's Code" (Ron alludes to Ronald Rivest). RC6 improved the design of RC5 by introducing an additional data-dependent rotation multiplier, increasing encryption complexity & security. It is a block cipher & works with a block size of 128 bits & keys can be 128, 192, or 256 bits long.

Key features of the RC6 include:

- Using integer multiplication: This provides additional non-linearity compared to exclusive bitwise OR (XOR) & bitwise shifts.
- Data dependent rotations: Rotation (circular motion) depends on the data being encrypted, making it more complex & resistant to certain types of cryptographic attacks.
- Key-dependent S-Boxes: S-boxes (substitution boxes) depend on the secret key, which increases the security of the algorithm against attackers.
- Four data blocks: Plaintext & ciphertext are divided into four data blocks, as opposed to the two blocks used in RC5.[8]

In terms of execution, RC6 is planned to perform well on both equipment & computer program stages & is known to be simple to introduce. In spite of these points of interest, RC6 was not chosen for the AES standard; the Rijndael cipher was chosen instep.

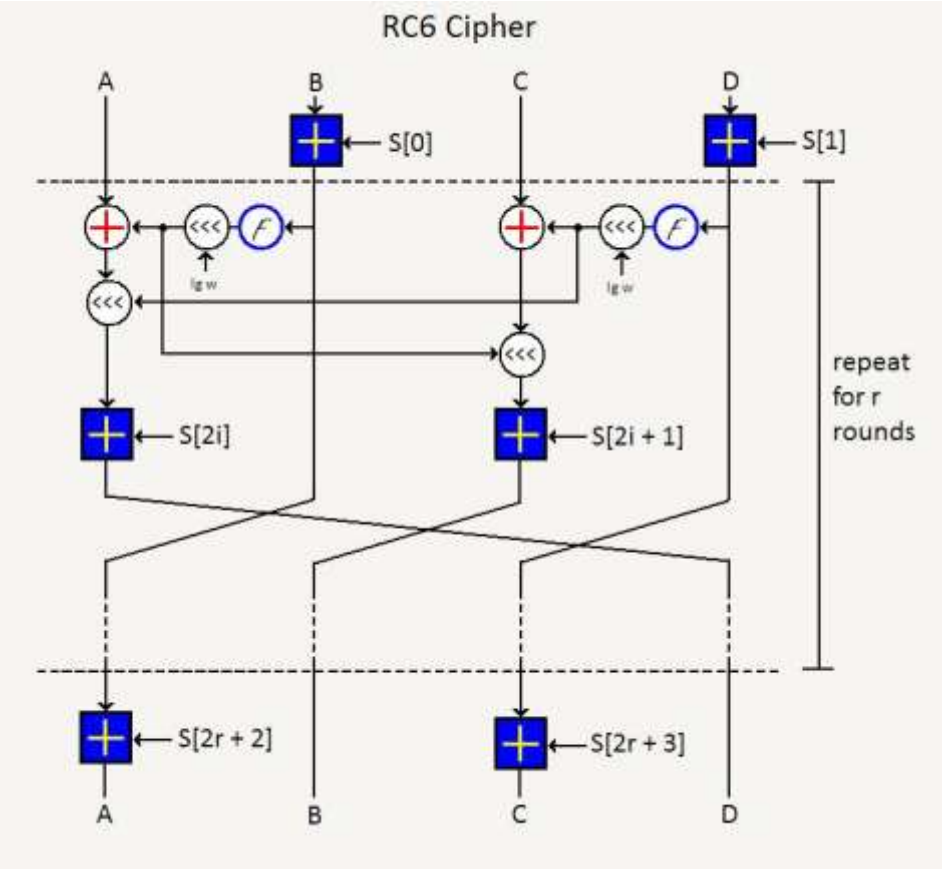


Figure 2:- RC6 Encryption

**3) "The Rijndael:-** The Rijndael cipher, also known as the "rain doll" or "SMKE cipher," was possibly developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, and uses symmetric key encryption. 2001. Rijndael cipher"[41] It has been designated as the Advanced Encryption Standard (AES) by the US National Established of Measures & Innovation (NIST).[4] Rijndael can be a block cipher with a block length of 128, 192, or 256 bits as well as the key length is also the same.. However, in the AES standard, the square estimate is 128 bits & the key estimate can be 128, 192, or 256 bits.[4][7]

This encryption method involves using a grouping of four rows & four columns of bytes known as a state. The encryption process consists of several distinct operational steps as below:

- Transformation by substitution of bytes. Typically, a substitution process that is not linear takes place in which every byte in the state is changed by a different byte that based on some specific substitution table known as an S-box.
- Rearrange the rows. This typically involves transposing each entry in the state table by a fixed number of steps each time it is pushed.
- Rearrange the order of the columns. By combining 4 bytes in the each of column, this procedure alters the arrangement of the state columns.
- Incorporate the Round_Key: During this stage, the circular key is merged with the state through the application of a bitwise XOR operation. The circular keys then derived by mixing key plot & the cipher key.
  - ✓ The size of the key determines how many Rijndael encryption cycles are needed: a 128-bit key requires 10 rounds, a 192-bit key requires 12 rounds & a 256-bit key requires 14 rounds.
  - ✓ Decoding is done by basically switching these steps.

AES (& by extension, the Rijndael cipher) is considered to be exceedingly secure & is broadly utilized universally for all sorts of touchy information encryption, counting government, commercial & individual applications.[4]

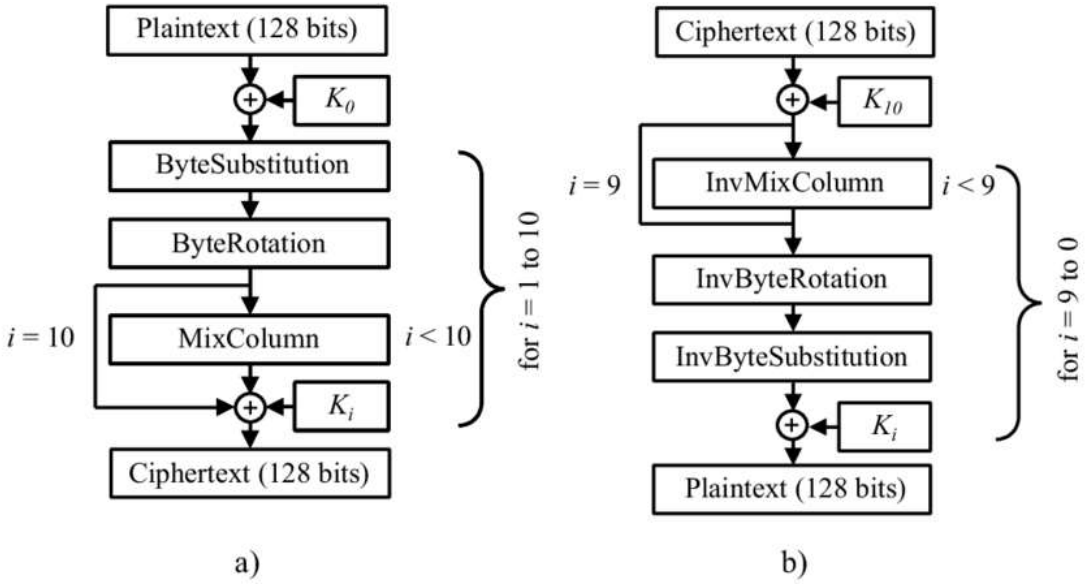


Figure 3:- The Rijndael Cipher Encryption & Decryption

**4) AES (Advanced Encryption Standard):-** "This could be a symmetric encryption computation created by the National Institute of Standards and Technology (NIST) in the United States in 2001"[41] Two [58] Belgian cryptographers, Vincent Rijmen [58] & Joan Daemen, submitted the winning algorithm in a public competition that resulted in the selection of AES. The created algorithm, formerly known as Rijndael, was chosen for its mix of security, performance, efficiency, simplicity of use, and flexibility.

In today's world, AES is frequently used to encrypt data, whether it be in files, communications, or protected systems.[17] Here is a general description of AES:

- Measure of the key utilized in encryption: The key sizes of 128, 192, & 256 bits are bolstered by AES. Choosing the fitting degree of security includes a compromise between security (since bigger measures are more secure) & execution (littler measures are speedier).
- Measure of the piece: The AES calculation works on 128-bit information squares, notwithstanding of the esteem of the key being utilized. On the off chance that the data that must be mixed isn't a diverse of the square appraise, it have to be be padded.
- "Circuits or cycles: The information encounters a number of stages of arranging, with [42] the number of rounds moving depending on the key gauge: 10 rounds for 128-bit keys,[42] 12 rounds for 192-bit keys & 14 rounds for 256-bit keys. Each cycle includes a few handling strategies, counting substitution, stage, blending & the expansion of circular components"[42]

AES works non-iteratively by rearranging & permuting bits. Calculations are performed on bytes instead of bits. A 128-bit plain content field is treated as 16 bytes organized in a 4x4 lattice. The key length decides the number of rounds required. Encryption & decoding are implemented separately, each happening within the handle of changing over plaintext to ciphertext.[9] AES scrambles each circular. The encryption prepare incorporates four subprocesses (subbyte, push move, column rearrange, circular key expansion).Decoding is additionally performed in each circular. It comprises of the same four subprocesses as encryption (subbyte, push move, column rearrange, circular key include), but wiped out switch arrange.

AES is the same as DES, but as innovation & information sizes increment, it employments more bits & DES doesn't have sufficient bits to scramble the information. It was not secure to fight off an "comprehensive key look assault". In other words, AES was presented with more bits than DES. AES scrambles information at 128 bits.

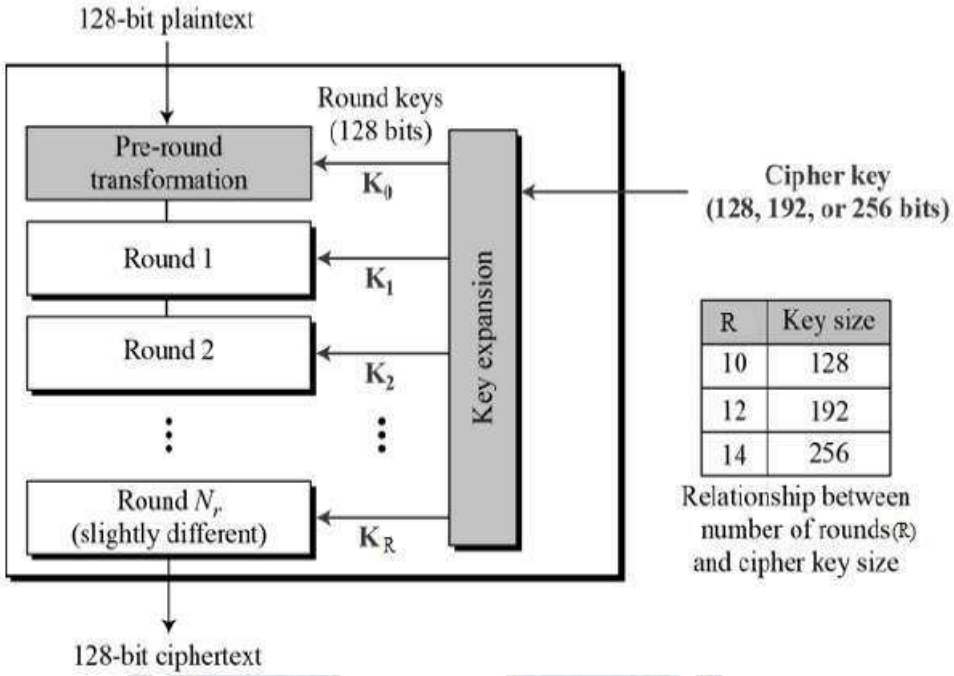


Figure 4:- Structure of AES

**5) Elliptic Curve Cryptography (EC&C):-** "Basically is a form of encryption using public key, it is based on the algebraic structure of elliptic curves over finite fields. This key cryptography differs that from others, like the RSA (Rivest-Shamir-Adleman), in that it provides the same level of security with less computing work & less resource consumption"[7][32]
Elliptic curves are mathematical constructs that can be described by this:

$$y^2 = x^3 + ax + b$$

There is only a limited, discrete range of potential values for x and y since the curves in the ECC context are over a finite field. The operations of the elliptic curve algebra are defined in terms of points on the curve. Importantly, it is computationally impossible to find n given a point P [39] & an integer n, while it is relatively easy to compute the point Q = nP by adding P to itself n times. This property serves as the foundation for ECC cryptography solutions.[30]
VPNs, secure mail, secure record exchange (SFTP), and secure web browsing are fair a number of of the applications that make utilize of ECC. Two well-known varieties are Elliptic Bend Diffie-Hellman (EC&DH) for key arrangement & Elliptic Bend Advanced Signature Calculation (ECD&SA) for advanced marks.
With ECDH, two parties can create a shared secret over an unprotected channel, with each party holding a pair of public & [57] private elliptic curve keys. This shared secret is used to generate the symmetric encryption key.[28]
The Advanced Signature Calculation (DSA), which utilizes elliptic bend encryption, incorporates a variation called ECDSA. ECDSA offers a strategy for a endorser to form a message's signature that a verifier may freely confirm to guarantee that the signature is honest to goodness & that the message hasn't been altered with, comparable to other advanced signature strategies.[35]
When compared to other types of public key cryptography, ECC offers a better balance between security & performance because its smaller keys yet guarantee the same level of protection. This causes computations to run more quickly & reduces network traffic. ECC is more difficult to accurately implement, though & ineffective implementations can leave systems open to a variety of assaults. It's crucial to constantly utilize reputable cryptography libraries & maintain them up to date.[33]

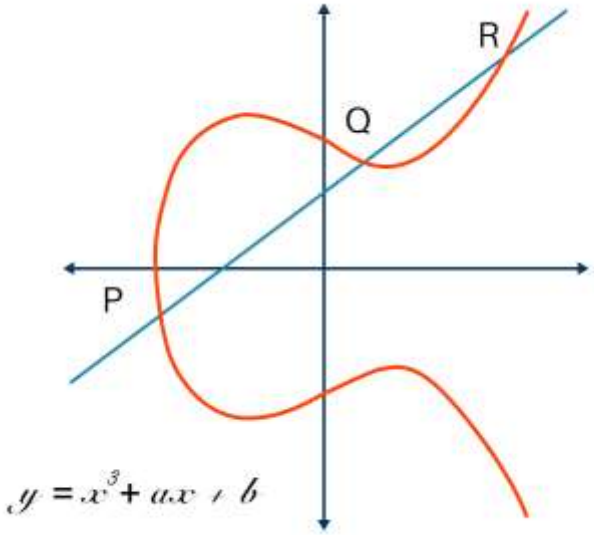


Figure 5:- Elliptic Curve Cryptography

6) **RSA (Rivest-Shamir-Adleman):-** RSA (Rivest-Shamir-Adleman) is a popular public-key cryptosystem that was developed in the early 1990s. The encryption key in such a system is made public, while the decryption key is kept hidden. This imbalance in RSA stems from the fact that factoring the product of two huge prime integers is notoriously difficult in practice.
The basic steps involved in RSA encryption & decryption are as follows:

- To Generate a Key: Pick any two prime numbers between 1 and 100. Choose p & q at random and make sure they have comparable bit lengths so that the product n = pq is more difficult to factor. It is important to conceal the actual p and q values.
- Compute n & ϕ(n): "The value n will serve as the modulus for both the public & private keys, hence it is necessary to calculate both n and (n). N is equal to p*q. In addition, the totient ϕ(n) = (p-1)*(q-1) is calculated for use in the key generation process"[52]
- Choose an integer e: Pick an integer e, where e is a positive number larger than 1 but less than ϕ(n). Coprimeness between e & ϕ(n) means that they have no common components larger than 1. The public key consists of the two numbers (n, e).
- The congruence relation d*e ≡ 1 (mod n) may be satisfied by computing d as follows. In essence, d is the multiplicative inverse of e modulo ϕ(n) in the modular setting. Therefore, d is the least positive integer that multiplied by e, modulo ϕ(n), solves the equation. The secret decoder is the pair (n, d).

  Encryption: Encryption is performed as follows, given a plaintext message m & the public key '(n, e)': Using a predetermined reversible protocol, or padding scheme, transform the plaintext into an integer in the range '[0, n-1)'. Using the formula c ≡ m^e (mod n), encrypt the padded message m to a ciphertext c ≡ m^e (mod n).
  Decryption: The decryption procedure, assuming the ciphertext c & private key (n, d), is as follows: From the ciphertext c, derive the padded message m using the formula m ≡ c^d (mod n). To recover the original, unencrypted message m, one must revert back to the encryption's padding technique. When big primes are used for p & q, RSA encryption provides a safe technique of encryption. Its safety arises from the fact that multiplying two huge primes together is computationally trivial, but factoring back into the original primes is computationally very complex. RSA is used for a broad variety of purposes, including sending encrypted emails & logging onto secure remote accounts.

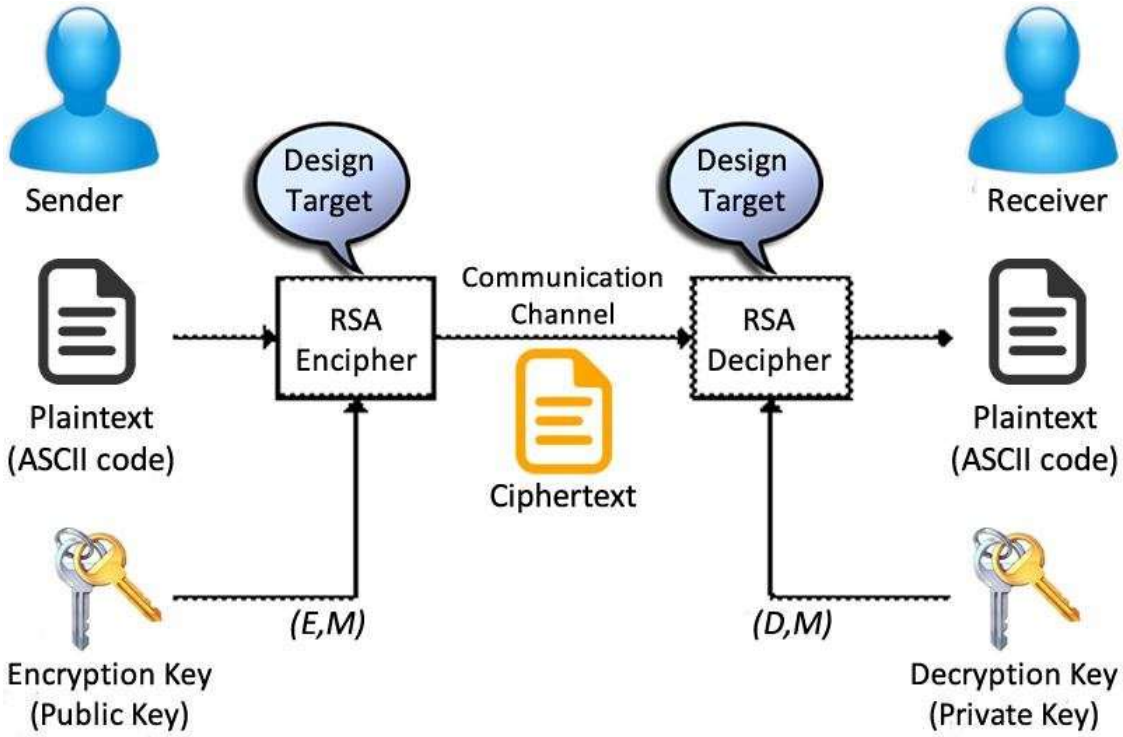


Figure 6:- RSA Algorithm

7) **SHA (Secure Hash Algorithms):-** U.S. Federal Information Processing Standard (FIPS) 199 specifies the Secure Hash Algorithms (SHA), a series of cryptographic hash functions developed & released by NIST. In cryptography, an input is processed by a mathematical procedure called a hash function, [46] which then outputs a string of bytes of a certain length. Typically, the result is a 'digest' that is specific to the given input. A new hash value should look unrelated to the previous one even when only a slight modification in the input is made.
Over the years, several variants of SHA have been created:

- The Secure Hash Algorithm (SHA) was first released in 1993 & its first implementation, SHA-0, used 160 bits. It had fatal defects, thus it was taken out of circulation.[47]
- The Secure Hash method 1 (SHA-1) is a hash function of 160 bits that is similar to the older MD5 method. The NSA developed this as a component of the Digital Signature Algorithm. Researchers have shown both theoretical & actual flaws & as a result, its use is being phased out.
- The SHA-2 family consists of two related hash algorithms, SHA-256 & SHA-512, with distinct block sizes. SHA-256 operates with 32-byte words, while SHA-512 operates with 64-byte words. “Each hashing standard also has shorter "truncated" variants: “SHA-224, SHA-384 [51] SHA-512/224 & SHA-512/256”
- The Secure Hash Algorithm 3 (SHA-3) was formerly known as Keccak; it is the newest addition to the SHA family & is distinct from SHA-2. In contrast to SHA-2, it is resistant to length extension attacks. This is a known flaw in SHA-2.

TLS/SSL, PGP, SSH, IPsec & Bitcoin are just a few of the many security protocols & programs that rely on SHA functions. Data integrity protection is their key use case in these contexts. To see if a file you downloaded has been tampered with in transit, you may, for instance, compare its SHA hash to the one supplied by the sender.
Step-by-step, here's how hash algorithms like SHA-1 are constructed:

- Preprocessing: The input message is padded before processing so that its final length is 448 modulo 512. No matter how long anything is, padding is always added. This padding is a 64-bit big-endian integer that begins with a 1[49], “followed by as many zeros as needed to attain the [55] desired length & finally the length of the input message”
- Dividing: 512-bit (64-byte) divisions make up the padded message.
- Initialize Hash Value: The hash value is initialized with a set of five constants, each of which is 32 bits in size.
- Processing: In order to generate a 160-bit output hash, the hash value & block data are subjected to a series of bitwise operations, logical functions & modular arithmetic as they are processed one by one.[50]

These hash functions are intended to be both quick & safe. Instead of encrypting or creating secret keys, they are designed to create a one-of-a-kind & unchangeable representation of data.

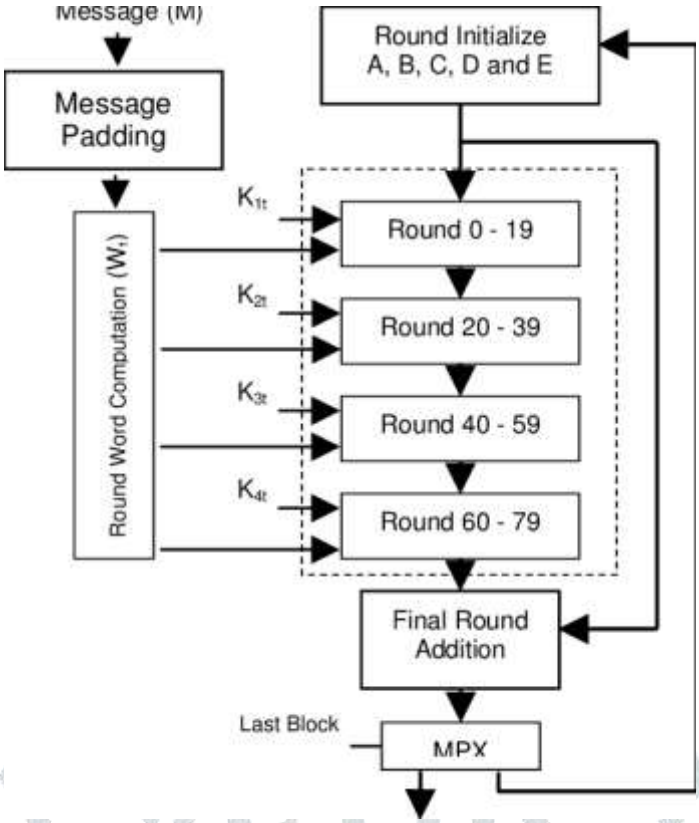


Figure 7:- SHA Algorithm

8) **Homomorphic Encryption Standard:-** "When decoded, the encrypted result of a computation on the ciphertext is the same as the result of the same operations on the plaintext; this sort of encryption is known as homomorphic encryption. For safe, private calculations & transactions, the ability to execute encrypted data without first decrypting it might be immensely valuable.

Cloud computing is a key use case for homomorphic encryption since it's helpful to be able to work with data while it's still encrypted. Homomorphic encryption, for example, may help medical researchers study patient data without compromising confidentiality.

Different homomorphic encryption systems exist, each with its own set of advantages & disadvantages:-

- Partially Homomorphic Encryption (PHE): Systems that use partially homomorphic encryption (PHE) are able to repeatedly carry out a single operation, such as addition or multiplication, indefinitely. PHE is shown by RSA.
- "Somewhat Homomorphic Encryption (SHE):SHE, or somewhat homomorphic encryption,[54] is a kind of encryption that allows for restricted iterations of addition & multiplication operations".
- Fully Homomorphic Encryption (FHE): Using Fully Homomorphic Encryption (FHE), "the ciphertext may be added & [56] multiplied an infinite number of times without revealing any information. Craig Gentry introduced the first FHE plan in 2009"[53]

The computational efficiency of homomorphic encryption systems is a major difficulty. In particular, FHE is currently seen as too computationally costly for most practical applications. But researchers are attempting to improve the effectiveness & practicality of these methods".[44]

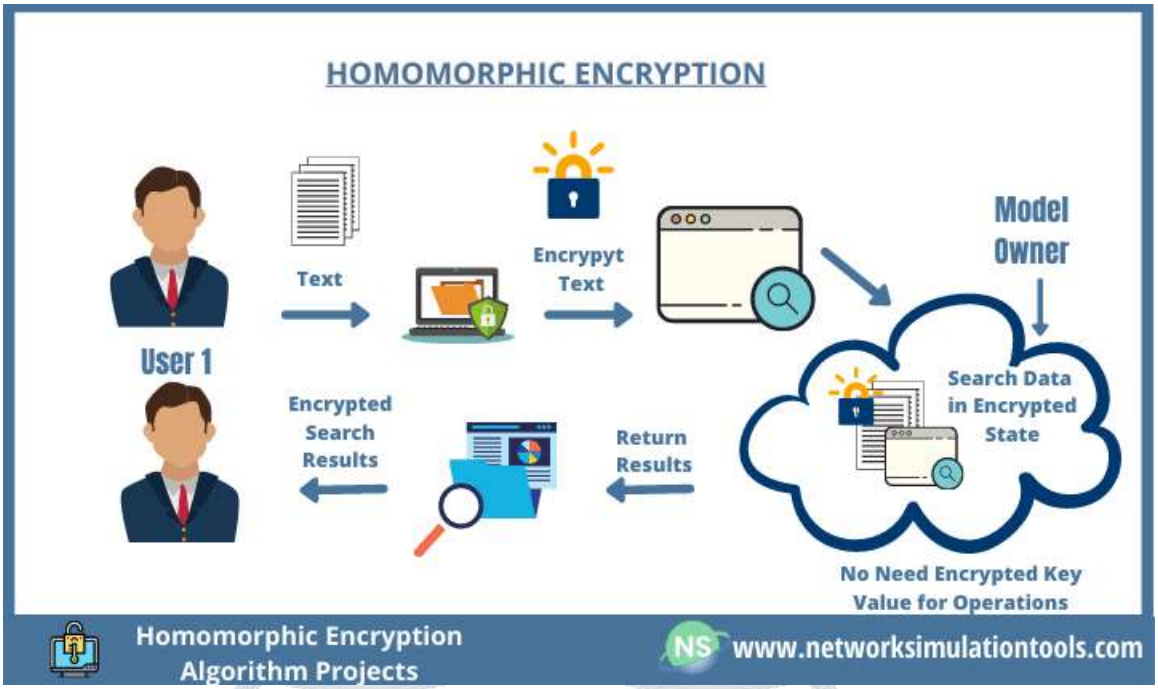


Figure 8:- Homomorphic Encryption Standard

## 3. Conclusion

In today's profoundly computerized & quickly advancing world, the significance of encryption & unscrambling strategies is basic. Serving as the essential defense against unauthorized information get to, these cryptographic components are an indispensably component in keeping up protection & information security. The wide extend of calculations advertised by symmetric and topsy-turvy key cryptography, such as AES, DES, RSA & ECC, frame a flexible arms stockpile for defending computerized data's realness, secrecy & keenness. Their application ranges over different spaces, from giving secure computerized marks & information transmission to secrecy confirmation & secure key trades in cloud computing settings. By the by, choosing an encryption approach requires cautious thought of a few components, adjusting the requests of security, computational effectiveness & execution capabilities. It's worth noticing that no encryption strategy is impenetrable to all dangers. With the persistent advance in computing control and the development of unused security dangers, the range of cryptography requires constant investigate & advancement. Additionally, it is pivotal to get it that encryption shapes as it were one viewpoint of a comprehensive security arrange. In spite of its necessarily part, it ought to be reinforced with solid security conventions, hones & foundations for ideal adequacy. In outline, as we move assist into the advanced age & with the developing dependence on cloud computing, the centrality of encryption & unscrambling techniques is bound to extend. Their able and viable utilization will be imperative in protecting security, believe & security in our computerized communications & exchanges.

## 4. Future Work

The domain of encryption & decryption methodologies is wide-ranging & constantly progressing. Here are some potential areas for development & exploration in this sector:-

- Quantum Cryptography: Considering the potential capabilities of quantum computers to effortlessly crack existing encryption algorithms, developing new methods of encryption resilient to quantum computer attacks is an important area of focus for the future. Quantum key distribution (QKD), a technique allowing the generation of a random secret key known only to the participating parties, holds promise in this area.
- Lightweight Cryptography: The rise of Internet of Things (IoT) devices, which typically have limited computational capabilities & energy reserves, necessitates the development of lightweight encryption algorithms. These algorithms must be secure, while also requiring minimal resources for implementation & operation.
- Post-Quantum Cryptography: In view of the quantum computing threat, research into post-quantum cryptography – cryptographic algorithms that are considered secure against quantum computer attacks – is gaining more importance.
- AI & Machine Learning in Cryptography: Emerging research is exploring how AI & machine learning can be utilized to enhance encryption methods, identify anomalies, thwart attacks, or even devise new encryption algorithms. Conversely, ensuring the secure use of AI, including the protection of data privacy during AI model training & deployment, is also a significant concern.
- Privacy-Preserving Techniques: Methods such as differential privacy, which provide robust privacy assurances, could be amalgamated with encryption for data protection. Future work could involve the development of practical & efficient systems offering both encryption & differential privacy.

- Blockchains & Cryptocurrencies: Cryptographic algorithms form the bedrock of blockchain technology & cryptocurrencies such as Bitcoin. Future research could concentrate on designing cryptographic protocols for these systems that are more secure, efficient & scalable.
- Biometric encryption: An individual's fingerprints or a scan of their face are used in biometric encryption to generate a secret key. Mobile phones & other personal electronic devices are rapidly adopting this technology because it is more secure than password-based encryption. A person may unlock their cellphone by scanning either their fingerprint or facial features. The biometric information is then used by the gadget to unlock the data's encryption key.
- Hardware-based encryption: Hardware-based encryption relies on specific hardware to perform the tasks of encrypting & decrypting data. This method of encryption is preferred in highly sensitive environments like financial & military networks because it is more robust than software-based alternatives. Hardware encryption is more secure since the encryption key is held on a protected chip rather than in software.

## 5. Further References

[1] Mell, P., & Grance, T. in 2011. NIST Cloud Computing Definition. Nationally Prepared for Guidelines & Innovations, 51(7), 55.
[2] Stalling, W. in 2017. Organizing encryption & security: Standard & Hone. Pearson.
[3] Singh, S., Jeong, Y.S. & Stop, J. H. in 2016. Cloud Computing Security Overview:
Problems, dangers & rules. Journal of Arrange & Computer Applications, 78, 202-224.
[4] Daemen, J. & Rijmen, V. in 2002. The Rijndael Plan:AES is an advanced encryption standard. Springer Scientific & Commercial Media.
[5] Rivest, R.L., Shamir, A. & Adleman, L. in 1978. A strategy for obtaining advanced tokens & public key cryptosystems. Communications of the ACM, 22(4), 122-128.
[6] Schneier, B. (1996). Encryption enabled: conventions, calculations & source code C. John Wiley & Children.
[7] Huang, Y., Yu, FR, Liu, C., Xie, S., and Chouinard, JY in 2004. An overview of organizational testbeds typical of large-scale applications (SDN): Approaches & challenges. IEEE Communications Review & Training Exercises, 21(5), 892-918.
[8] Puthal, D., Sahoo, BPS, Mishra, S. & Swain, S. in the year 2015. Highlights, issues & challenges of cloud computing: a huge statue. In Computational insights in information mining (pp. 2-17). Sweater.
[9] Gu, L. and Li, H. in 2007. Security Issues in Cloud Computing and Countermeasures. in 2010 IEEE 3rd World Conference on Innovations in Broadband Organization and Interactive Media (IC-BNMT).
[10] Coppersmith, D. in the year 2000. The effectiveness of the information encryption standard (DES) against attacks. IBM Journal of Research & Development, 41(5), 242-251 .
[11] Rivest, R. L., Sidney, R., Yin, YL ir Robshaw, M. in 1998. Het RC6-vierkantcijfer. RSA Research Facilities Accommodation at 56 TTW.
[12] Nationally organized benchmark and innovation. In 2001. Progressive Encryption Standard (AES). Distribution of state data processing tools, 198, 4415.
[13] Ingrian Systems Inc. in the year 2001. Phases of DataSecure: Protect information in applications, databases & capacity systems. Retrieved from Ingrian Systems Inc. Chronicles
[14] SafeNet Inc. in 2009. SafeNet completes the protection of Ingra systems. Press Ignore. Retrieved from SafeNet Inc website.
[15] Gemalto in 2014. Gemalto completes purchase of SafeNet. Press Ignore. Retrieved from Gemalto website.
[16] Collected by Thales in the year 2019. Thales Adds Gemalto Security to Become Global Pioneer in Automated Security. Press Ignore. Retrieved from the Thales Bunch website.
[17] National Foundation for Guidance & Innovation (NIST) in 2001. Progressive Encryption Standard (AES). Dissemination of government data preparation guidelines. Retrieved from NIST website.
[18] National Organization for Standards & Innovation (NIST) in 1977. Information Encryption Standard (DES). Dissemination of government data preparation guidelines. Refreshing from the NIST site.
[19] Eastlake, D. & Jones, P. in the year 2001. US Secure Hash Calculation 1 (SHA1). RFC 3174. Retrieved from the Building Assignment Disk (IETF) website.
[20] Johnson, D. & Menezes, A. in 1993. Extended Elliptic Bending Signature Calculation (ECDSA). Universal Journal of Data Security.
[21] Katz, J. & Lindell, Y. in 2014. Introducing advanced encryption. print CRC.
[22] Schneier, B. in the year 1996. Encryption enabled: Contracts, Calculations & Source Code C. Wiley Distributing.
[23] Diffie, W. & Hellman, M. in 1976. Headers are not used in cryptography. IEEE Exchange on Data Hypothesis.
[24] Stallings, W. in 2013. Organizing encryption & security: Standard & Hone. Student lobby.
[25] Boneh, D. in 2001. Choosing a Diffie-Hellman problem. In Third Symposium on Algorithmic Numerical Hypothesis.
[26] Van Tilborg, H. C. & Jajodia, S. in the year 2011. A reference work on cryptography & security. Sweater.
[27] El Kaafarani, A. in 2020. Plans for the Web of Things' encryption. Springer.

[28] Menezes, A.; Johnson, D. in 1993. The digital signature algorithm with elliptic curves (ECDSA). Journal of Information Security International.
[29] Jones, P., & Eastlake, D. (2001). SHA1 is the US Secure Hash Algorithm. RFC 3174. Internet Engineering Task Force (IETF) webpage retrieved.
[30] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Strategy for Getting Computerized Marks and Public-Key Cryptosystems. Communications of the ACM.
[31] Katz, J., & Lindell, Y. (2014). Presentation to Cutting edge Cryptography. CRC Press.
[32] Boneh, D. (2001). The Choice Diffie-Hellman Issue. In Third Algorithmic Number Hypothesis Symposium.
[33] Van Tilborg, H. C., & Jajodia, S. (2011). Reference book of Cryptography & Security. Springer.
[34] El Kaafarani, A. (2020). Encryption Plans for the Web of Things. Springer.
[35] Diffie, W., & Hellman, M. (1976). Modern headings in cryptography. IEEE Exchanges on Data Hypothesis.
[36] Kunal Mahajan, Sunil Kumar, Dilip Kumar."Chapter 45 Hybrid Methods for Increasing
Security of IoT and Cloud Data", Springer Science and Business Media LLC, 2023
[37] Marie A Wright. "The Advanced Encryption Standard", Network Security, 2001
[38] Student paper AES ,"Submitted to University of Bath'
[39] Rangel, Denise A. "Elliptic curves and factoring", Proquest, 20111108
[40] https://www.wikimili.com/
[41] https://www.northampton.ac.uk/research/faculty-research/
[42] https://www.vibdoc.com/
[43] https://www.nanopdf.com/
[44] https://www.news.ycombinator.com/
[45] https://www.nshielddocs.entrust.com/
[46] "Towards Digital Signatures and Public-Key Systems: An Approach." The groundbreaking work by Rivest, Shamir, & Adleman was published in Communications of the ACM, volume 29, issue 7, 1980, on pages 80–90. This pioneering paper was the debut of the RSA algorithm to the world.
[47] "Compendium of Applied Cryptography." Menezes, van Oorschot, & Vanstone's authoritative text was issued by CRC Press in 1996. An extensive study of the RSA algorithm is found in Chapter 12 of this extensive cryptography guide.
[48] "An Introduction to Cryptography: Principles and Applications." This exploration of cryptography, including the RSA algorithm, was authored by Delfs & Knebl and published by Springer in its 4th Edition in 2017.
[49] RSA Laboratories. "Deciphering RSA." Available online. This digital resource from RSA, the firm formed by the creators of the RSA algorithm, provides insight into RSA's operation and practical applications.
[50] National Institute of Standards and Technology (NIST). "Government-Approved Elliptic Curves." Accessible online. This online guide provides an outline of cryptographic algorithms, including RSA, endorsed for use by the federal government.
[51] Christoph Dobraunig, Maria Eichlseder,Florian Mendel. "Chapter 25 Analysis of SHA512/224 and SHA-512/256", Springer Science and Business Media LLC, 2015.
[52] Roop Kamal Kaur, Kamaljit Kaur. "A New Technique for Detection and Prevention of Passive Attacks in Web Usage Mining" , International Journal of Wireless and Microwave Technologies, 2015.
[53] Bineet Joshi, Bansidhar Joshi, Anupama Mishra, Varsha Arya, Avadhesh Kumar Gupta, Dragan Peraković. "A Comparative Study of Privacy-Preserving Homomorphic Encryption Techniques in Cloud Computing" , International Journal of Cloud Applications and Computing, 2022.
[54] N. Sheena, Shelbi Joseph, Shailesh Sivan, Bharat Bhushan. "Light-weight privacy enabled topology establishment and communication protocol for swarm IoT networks" , Cluster Computing, 2022.
[55] Raffaele Martino, Alessandro Cilardo. "A Flexible Framework for Exploring, Evaluating, and Comparing SHA-2 Designs" , IEEE Access, 2019.
[56] Bineet Joshi, Bansidhar Joshi, Anupama Mishra, Varsha Arya, Avadhesh Kumar Gupta, Dragan Peraković. "A Comparative Study of Privacy-Preserving Homomorphic Encryption Techniques in Cloud Computing" , International Journal of Cloud Applications and Computing, 2022.
[57] Guma Ali, Mussa Ally Dida, Anael Elikana Sam. "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications" , Future Internet, 2021.
[58] Marie A Wright. "The Advanced Encryption Standard" , Network Security, 2001.