IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, May 2024

Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations

Somnath Banerjee

Data Engineer, AMFAM ,Madison, USA

Abstract: *This paper examines various significant symmetric and asymmetric cryptography algorithms and their importance in network security. With the increasing use of the internet, there has been a corresponding rise in attacks on communication channels. Such attacks may enable third parties to access sensitive information regarding an organization and its operations. This information could potentially be used to disrupt an organization's activities or to extort payment in exchange for the data. To mitigate these risks, cryptographic algorithms are employed to secure communications. These algorithms encrypt data in a manner that makes it difficult for unauthorized individuals to access, rendering it ineffective for attackers. Consequently, these algorithms are essential to the security of communications. This paper presents a study of symmetric and asymmetric algorithms with respect to optimal resource allocation, potential attacks that may exploit these algorithms, time and power consumption, overall structure, and other relevant factors, along with an explanation of various security attacks.*

Keywords: CIA triad, NIST, FIPS, eavesdropping, DES, AES, RSA, ECC, Symmetric cipher, Asymmetric cipher

I. INTRODUCTION

In the current landscape, data is a valuable asset. It provides insights into an organization’s strengths and weaknesses. Those who can acquire and analyze this data using statistical or logical methods can influence organizational activities, either directly or indirectly. This raises the question of whether security measures should be implemented for this important asset. Cryptography addresses this need by securing information and communication through techniques based on mathematical principles and algorithmic rules. An effective cryptography method would allow access to the data only for those individuals for whom the information is intended.[1][2][3][4].

Cryptography goals

The primary objective of cryptography is to protect information from being understood by unauthorized individuals who should not access the message. This objective can be further divided into several sub-goals.[2] These are listed below

Confidentiality:

This term encompasses two related ideas: Data confidentiality: This principle ensures that personal data is accessible only to those who are authorized. Privacy: This principle guarantees that the information gathered is provided solely to the intended recipients and is not disclosed beyond that.

Integrity:

Integrity encompasses two related concepts:

Information integrity: This refers to the modification of information in a specified and approved manner.

System integrity: This ensures that a device or software operates reliably, without unauthorized manipulation, whether intentional or accidental.

DOI: 10.48175/IJARSCT-18097

Availability:

Ensures that systems function as intended and that repairs are accessible to authorized users. The objectives mentioned above are referred to as the CIA triad. These three concepts represent the essential security objectives for information and computational services. For instance, the NIST standard FIPS 199 (Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems) identifies confidentiality, integrity, and availability as the three security objectives for information and information systems. FIPS 199 offers a useful characterization of these objectives in terms of requirements and the definition of a security loss in each category: [3][1]

Confidentiality: established restrictions on information access and disclosure to protect personal privacy and proprietary information.

Integrity: safeguarding against unauthorized alterations or destruction of information, ensuring that the information remains reliable and credible. Unauthorized manipulation of information results in a loss of integrity.

Availability: ensuring timely and reliable access to and use of data. A loss of availability refers to the disruption of access to data or related systems.

While the use of the central intelligence agency triad to outline security objectives is well established, some in the security field believe that additional components are needed to provide a comprehensive view. Two of the most commonly mentioned areas are as follows: [1][3][4]

Authenticity refers to the quality of being genuine and capable of being verified and trusted. It involves confidence in the validity of a transmission, a message, or the originator of that message. This means that users are identifiable as they claim to be, and the information entering the system originates from a reliable source.

Accountability pertains to an entity's responsibility to an authority regarding any loss or misuse of information. Given that fully secure systems have not yet been realized, it is essential to trace any security breach back to a responsible party. Systems should maintain records of their activities to assist forensic analysts in investigating security breaches or resolving transaction disputes.

How does cryptography work?

There are two individuals, Alice and Bob, who want to communicate and share information about the future ambitions of their company. They are using a standard communication channel that is not secure. Since this information is important for the company’s future operations, it needs to be safeguarded. If Oscar, who is not intended to receive this information, acquires it through eavesdropping methods and decides to undermine their objectives, he could potentially distort the data by misappropriating their intellectual property and selling it to others.[2][4]

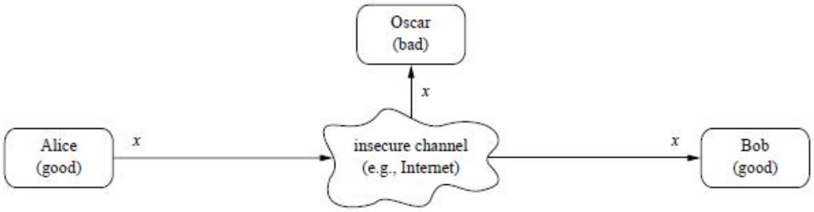


Fig 1. Communication Over an insecure Channel [2]

Cryptography can reduce such risks. The symmetric cipher, which has been extensively modernized, is a basic type of encryption method where one secret key is shared through a secure channel between Alice and Bob before their communication starts. This secure channel could be a face-to-face meeting or another method. The sender uses this key to encrypt the message, while the recipient uses it to decrypt the data. Plain text refers to unencrypted data, whereas cipher text refers to encrypted data. Even if Oscar intercepts their conversation, he would not be able to decipher the message because it is encrypted with a secure key known only to Alice and Bob. Consequently, all essential data will be safeguarded, and if someone gains access to critical messages, they will be unable to decrypt them without the private key, which will be held exclusively by the intended recipients.[2][3]

DOI: 10.48175/IJARSCT-18097

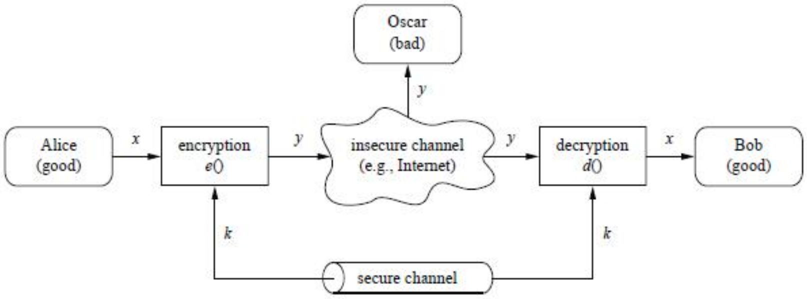


Fig 2. Symmetric-key cryptosystem [2]

- x is called plain text
- y is called ciphertext
- k is called private/secret key
- the set of all possible keys are called key space

The important point to consider is that the private key should remain confidential, while the algorithm can be shared publicly. Maintaining the confidentiality of the method can help prevent unauthorized parties from decrypting communications, but keeping the algorithm private may suggest that it has not undergone thorough testing. Sharing an encryption method's algorithm with the cryptographic community allows for assessment of its strength and resilience against potential attacks. The private key is the only element that needs to be kept hidden.

Remark

The primary focus here is confidentiality, which involves concealing the contextual meaning of the message from individuals who do not have authorization. Cryptography can also serve to prevent unauthorized third parties from making unnoticed alterations to the data (ensuring message integrity) or to confirm that the data originates from a verified user (ensuring message authenticity)

Types of cryptography

There are mainly two types of cryptography:-

1. Symmetric cipher : DES, AES
2. Asymmetric cipher : RSA, ECC

Symmetric cipher

The symmetric cipher uses a single private key for both data encryption and decryption. If Alice wishes to send a message to Bob, she can use the K1 private key, which will also be utilized by Bob to decrypt that message. [2][3]

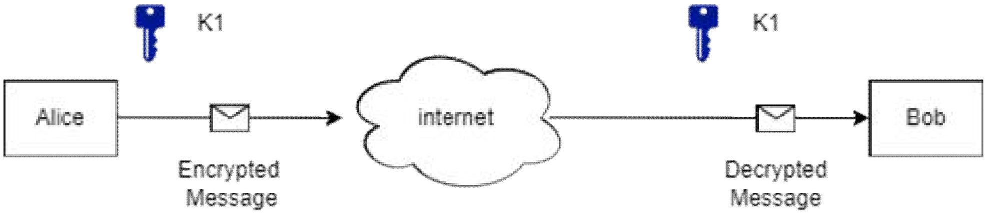


Fig 4. Symmetric encryption between 2 users[5]

If a third party, such as Charlie, wants to send a message to Alice, it is advisable to use a different key than K1. K1 is already being used for secure communication between Alice and Bob, meaning that Bob can decrypt any messages intended for Alice because he possesses that key. To avoid this situation, it is important for each pair of individuals on the network to communicate using a unique key. The same principle applies to establishing a connection between Charlie and Bob.

DOI: 10.48175/IJARSCT-18097

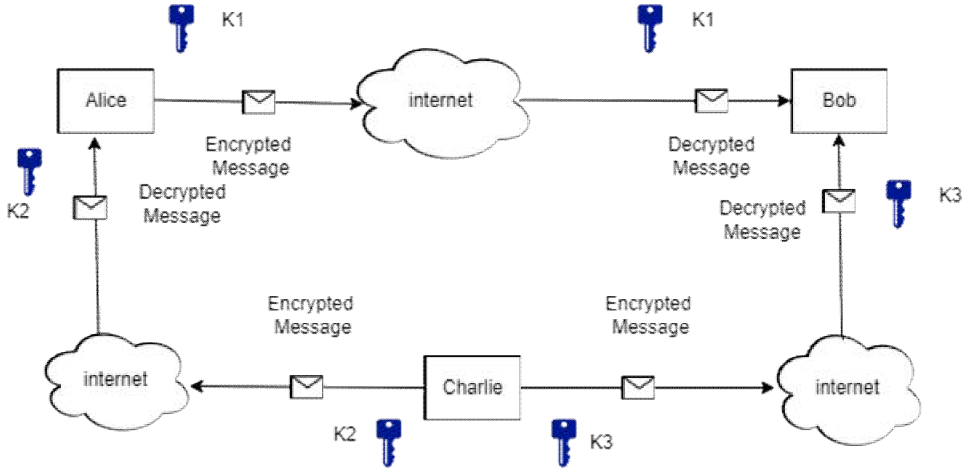


Fig 3. Symmetric encryption among more than 2 users[5]

Drawbacks: The main drawback of symmetric encryption is the growing number of unique keys needed to communicate with multiple users. For example, if one individual needs to communicate with 100 others, they must manage and secure 100 keys, complicating the encryption process. Another significant disadvantage of symmetric encryption is that the private key must be shared between both parties to ensure secure communication. There is no electronic communication method that can guarantee absolute security.

Asymmetric Cipher: To address the limitations of symmetric encryption, the asymmetric cipher was introduced by Whitfield Diffie and Martin Hellman in 1977, commonly referred to as public-key cryptography. This method utilizes two keys instead of just one. Similar to symmetric encryption, one key is private, while the other is public and accessible to all members of a network. When data is encrypted with a public key, it can only be decrypted with the corresponding private key. Conversely, if a private key is used to encrypt data, the associated public key is used for decryption. This process ensures that the sender is always verified. The public key encrypts the message based on the recipient's private key and vice versa. For instance, if Alice wants to send a message to Bob using asymmetric encryption, she must encrypt the message with Bob's public key, which can only be decoded with Bob's private key, known only to him. Consequently, each connection does not require a unique key but rather a single unique key for anyone on the network, along with a public key accessible to all. The same process applies if Charlie sends a message to either Alice or Bob.[2][3]

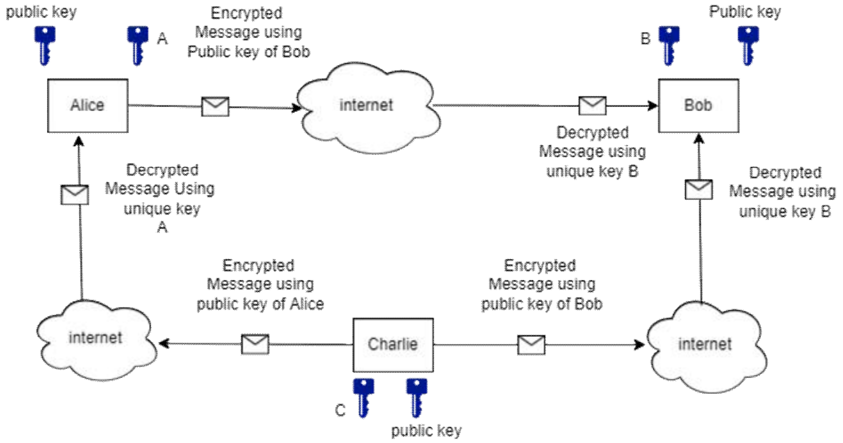

public key
A
Encrypted Message using Public key of Bob
B
Public key
Alice
internet
Bob
Decrypted Message using unique key B
Decrypted Message Using unique key A
Decrypted Message using unique key B
Encrypted Message using public key of Alice
Encrypted Message using public key of Bob
internet
Charlie
internet
C
public key

Fig 5. Asymmetric encryption[6]

DOI: 10.48175/IJARSCT-18097

Advantages Over Symmetric Encryption

- The key distribution problem has been addressed. As there is no requirement to transmit secret keys, this method is considered more secure than symmetric encryption. The use of digital signatures is permitted, enabling the recipient to verify the source of the message, thus ensuring message authenticity. It also facilitates non-repudiation, meaning the sender cannot deny having sent a message

Disadvantages:

- It is a relatively slow process, making it less suitable for decrypting large volumes of messages. If an individual loses their private key, they will be unable to decrypt their messages. If an unauthorized party gains access to someone's private key, they can potentially read their messages.

Operation of Algorithms for Data Encryption Standard (DES)

DES stands for Data Encryption Standard. It is an algorithm of symmetric cryptography. DES is a block cipher and encrypts data in blocks of size 64 bit. There are a few steps to understand how DES works. [5][6]

Operations on message:

1. Initial permutation: In this the 64 bit block data is handed over to an initial permutation function.
2. In the second step, 64 bit data is again permuted into two blocks of 32 bit data. These blocks are called left plain text (LPT) and right plain text (RPT).
3. These both blocks are operated in a total of 16 rounds with a private key.
4. Final permutation is performed. This permutation is also called inverse initial permutation.

Operations on key:

1. Initially the key size is 64 bit.
2. 8 Parity bits (8, 16, 24, 32, 40, 48, 56, 64) are removed and the key size becomes 56 bits.
3. These 56 bits will be divided into two equal sized blocks of 28 bits each.
4. Left circular shift will be performed on the basis of the round number.

- If the round number is one of these (1, 2, 9, 16) there will be one bit circular shift.
- Else there will be a two bit circular shift.

1. A copy of both blocks of sub-keys will be used in the next round. For the current round the both sub-keys will be combined. This will give 56 bits sized sub-key for the round.
2. Now a permutation function will choose 48 bits from 56 bits and arrange them. It is called “Compression-Permutation operation”.

Core operations in each round:

1. Left plain text (LPT) block and one copy of right plain text (RPT) will be passed at the end..
2. Right plain text block will have bits expanded by expansion permutation. (from 32 bits to 48 bits)
3. This 48 bit block will perform XOR operation with the sub-key.
4. This 48 bit resultant block will be passed with substitution blocks (s-block) and ultimately turned into 32 bits block.
5. This 32 bit block will be again permuted.
6. This processed RPT will perform XOR with LPT.
7. The copy of initial RPT will work as LPT and processed RPT will be RPT for the next round.

DOI: 10.48175/IJARSCT-18097

II. PAGE LAYOUT

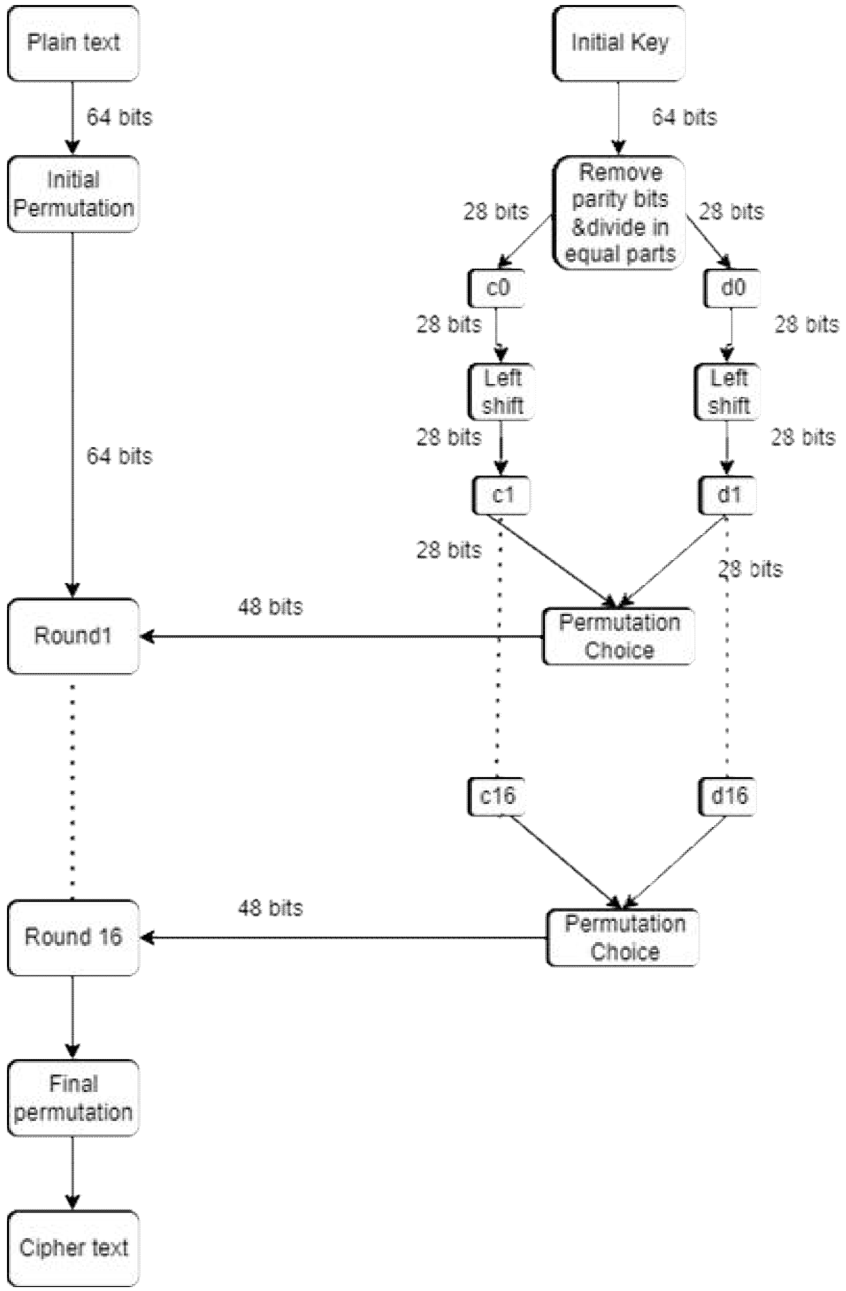


Fig 6. The layout of DES algorithm[6]

Substitution box operations:[10] [11]

1. 8 s-boxes work simultaneously to process 48 bits data blocks.
2. 6 bits are passed to each s-box.
3. First and last bit are combined. The decimal value of the obtained binary code will represent the number of rows. And the rest of the bits are combined whose decimal value will represent the number of columns.
4. Whatever data on that specific position in the initial 64 bit data table will be converted to 4 bits binary form.
5. Bits of this binary number will be output of s-box.
6. Every s-box will convert 6 bits into 4 bits. Hence 48 bits into 32 bits.

DOI: 10.48175/IJARSCT-18097

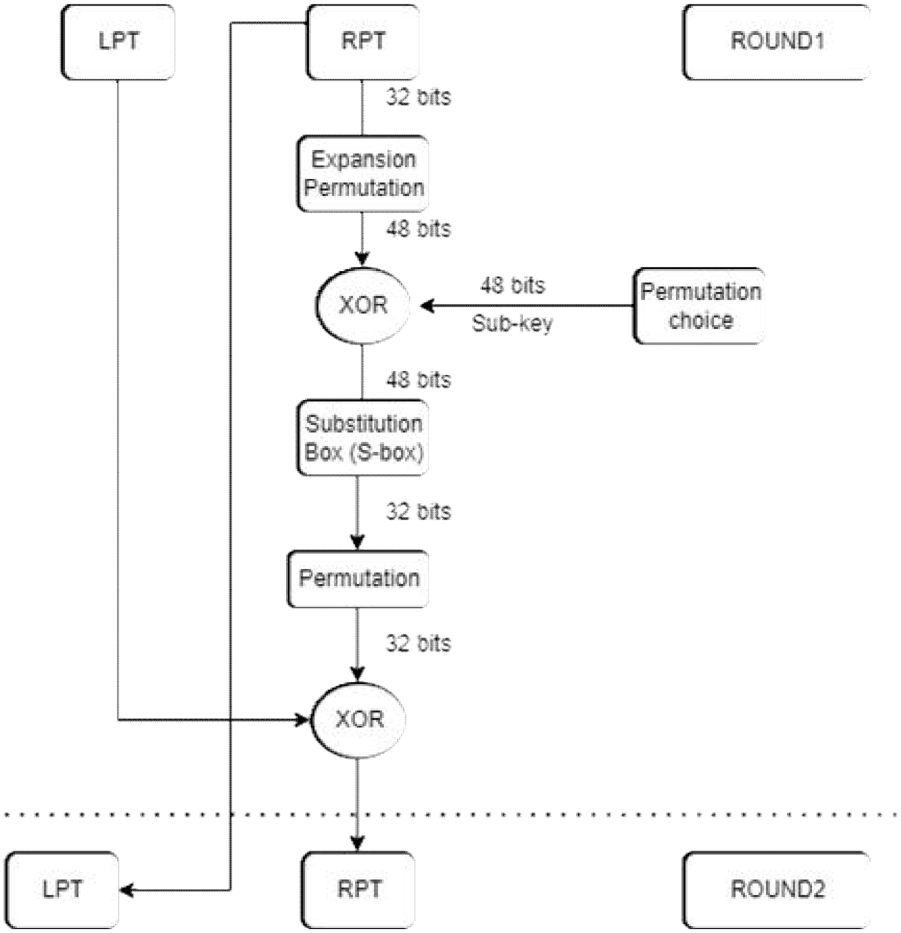


Fig 7. Internal working of DES[6]

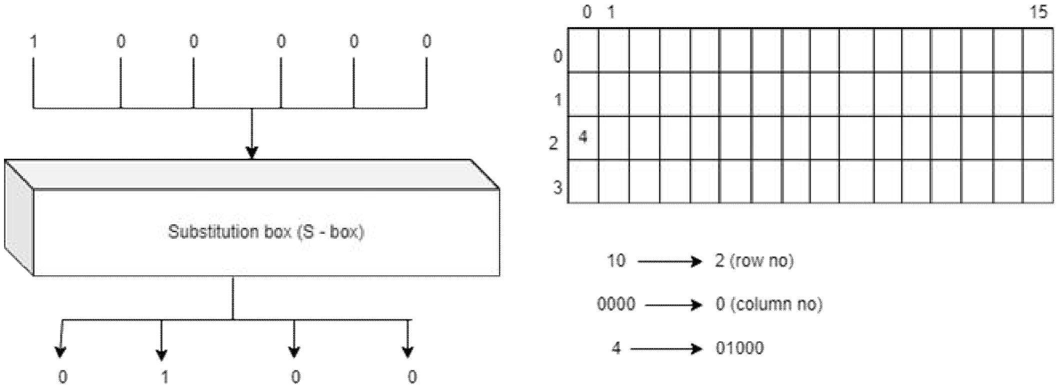


Fig 8. S-box illustration [10]

DES Limitations:

- **Key Size:** The sub-key is only of size 56 which results in 256 combinations, so even the brute-force attack is very efficient against DES encryption. Since modern computers have more computational power and they have the ASIC (application specific integrated circuit), it makes such computations much faster. [1][2] [8]

- **Weak keys:** 4 out of 256 combinations only contain 0's or 1's or half 0's and half 1's. The disadvantage of using weak keys is that, if we use weak keys in 2 continuous rounds, we get the same plain text we were processing. [9]
- **Semi-weak keys:** 6 out of these sub-key combinations will generate only 2 types of semi keys in 16 rounds. So each of them is repeated 8 times. So it will be easier for a cryptanalyst to decrypt the data.[2] [8]
- **Possible weak keys:** 48 key combinations are possible weak keys, which only generate 4 types of keys in 16 rounds. So each of them is repeated 4 times instead of having 16 distinct sub-keys.[2]
- **Key clustering:** If one sub-key k1 encrypts a message and some random key, k2 encrypts that message but it is the same as the initial message. This is called key clustering, which makes it weak algorithm to encrypt.[2]

Advanced Encryption Standards(AES)

AES stands for advanced encryption standards.

Operation on message: [9][11][12]

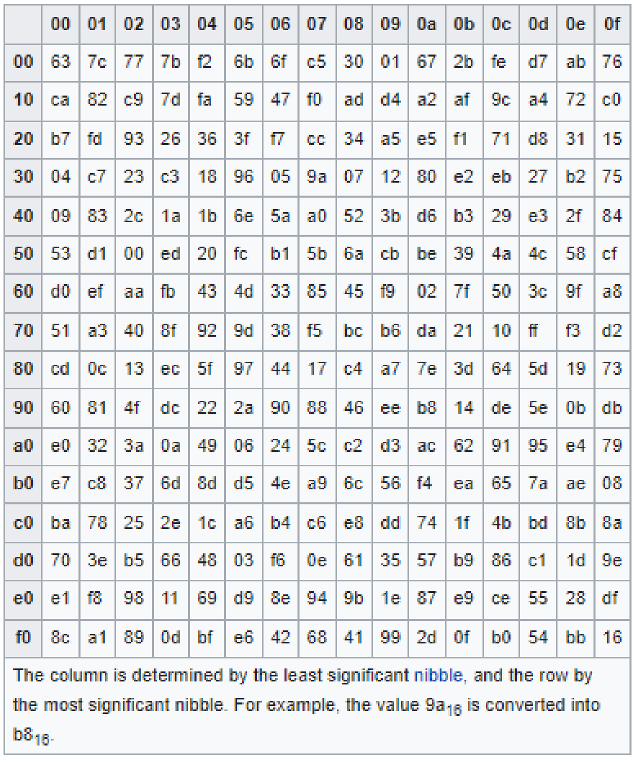
Whole message is divided into blocks of 128 bits.

- This 128 bits block would be in the form of a 4x4 matrix whose one cell would have size of 1byte (8bits).
- The block would be performing XOR operation with k0 sub-key and generate a state matrix. (intermediate form)

AES transformation function:

Sub-Bytes: State matrix will pass through the substitution box (Rijndael S-box). This s-box has a 16x16 matrix of distinct hexadecimal values.

Every cell of the data block will be replaced by these values. Every cell of data will have a hexadecimal value whose left digit will be denoting row no. and right digit will denote column number. Now the hexadecimal value at this specific position in s-box will replace value inside that state matrix.[12][13]



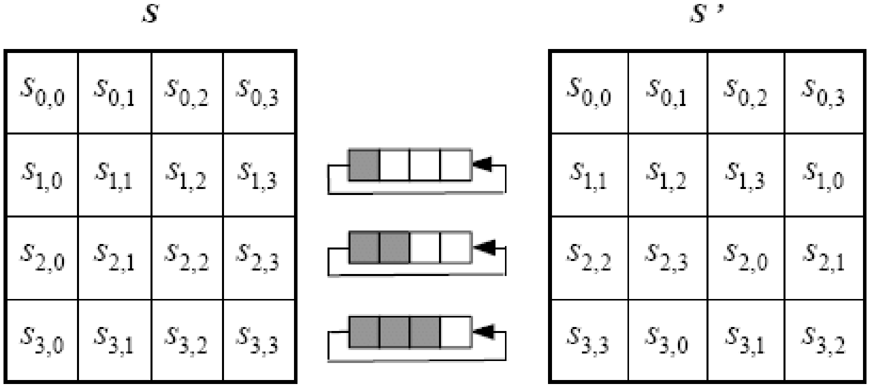
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

The column is determined by the least significant nibble, and the row by the most significant nibble. For example, the value $9a_{16}$ is converted into $b8_{16}$.

Fig 9. Rijndael S-box[12]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, May 2024

Shift Rows: State matrix will have it's rows shifted. First row will not be shifted. Second will shifted 1 time left side. Third row will shift 2 times to the left side. Fourth row will shift 3 times to the left side. [12][13]

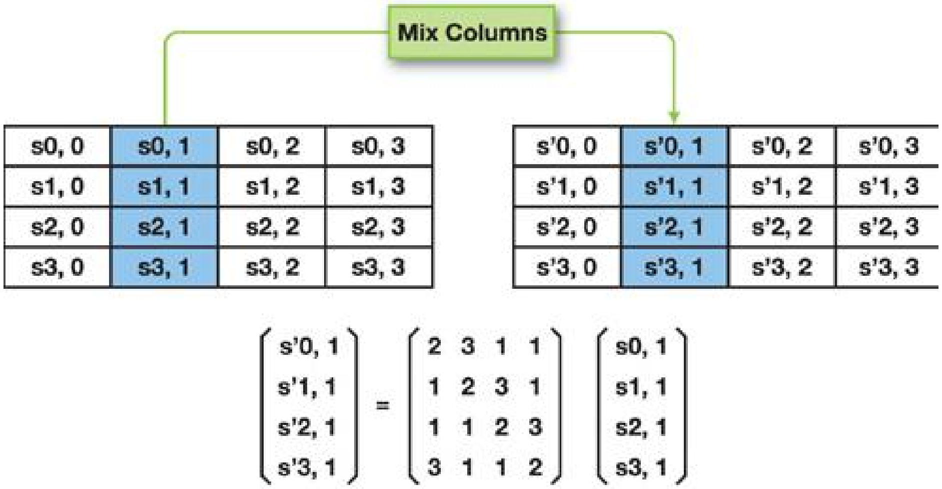


$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

Fig 10. Row shift step[13]

Mix columns: State matrix will be multiplied with a fixed 4x4 matrix. The only difference in this multiplication is changing normal addition (after multiplication) to XOR. In the last round this step is omitted. [12][13]



s0, 0	s0, 1	s0, 2	s0, 3
s1, 0	s1, 1	s1, 2	s1, 3
s2, 0	s2, 1	s2, 2	s2, 3
s3, 0	s3, 1	s3, 2	s3, 3

s'0, 0	s'0, 1	s'0, 2	s'0, 3
s'1, 0	s'1, 1	s'1, 2	s'1, 3
s'2, 0	s'2, 1	s'2, 2	s'2, 3
s'3, 0	s'3, 1	s'3, 2	s'3, 3

$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix}$$

Fig 11. Mix column[13]

Add round key: The last step is adding a rounding key with XOR operation.

Operations on key:

AES has 3 types of keys 128 bit, 192 bit and 256 bit. When we use a 128 bit key, 10 rounds are performed and 11 sub-keys are generated. When we use a 192 bit key, 12 rounds are performed and 13 sub-keys are generated. When we use a 256 bit key, 14 rounds are performed and 15 sub-keys are generated.
Key generator function is used to generate subkeys.
These sub-keys will be in the form of 4x4 matrices.

AES limitations:

- Uses too simple algebraic structure. [13]
- Every block is always encrypted in the same way. [12]
- Hard to implement with software. [13]
- Vulnerable to side channel attacks.

DOI: 10.48175/IJARSCT-18097

Rivest, Shamir and Adleman (RSA)

RSA stands for Rivest, Shamir, and Adleman algorithm. It is an asymmetric encryption technique which works on mathematical concepts of discrete logarithm. It also uses Trap-door functionality. In trap-door function it is easy to compute in one direction but to compute in reverse direction, we must have a trap-door value otherwise, it'd be extremely difficult to compute in the opposite direction. Here the trap-door value is "d" (decryption exponent). This is much like the normal logarithm, but the only difference is that only whole numbers are used and a modulus is involved. [14] [15]

Steps for RSA encryption:

Two random prime numbers are generated.

Let's suppose these two numbers are 2 and 7.

Multiply these two numbers and it will give us one number for the public key. This number will perform modulus with some other number.

$N = 2x7 = 14$

$\Phi(N)$ is calculated. ($\Phi(N)$ gives the number of co-prime numbers with N, from 1 to N).

$\Phi(14) = 6$.

Note: if we know the prime factors, it's just $(p-1)x(q-1)$. But since these two numbers are not disclosed with anyone, It takes excessive time to calculate it.

Choose a random number e (encryption exponent), which would be the second number of the public key. This number needs to be between 1 and $\Phi(N)$ and It must be coprime with N and $\Phi(N)$.

i.e. $1 < e < \Phi(16)$ and co-prime with 16 and 6.

In this case the number is 5.

Both numbers (5,16) work as public keys. Where any text will be converted to a number (can be based on position index of every alphabet) and this number will be raised to the power 5 and modulus 16.

Let's say we want to convert a message of one letter "b".

Index of b = 2

Expression to encrypt => 25(mod 16) = 4

4th index alphabet = "d"

So "b" is ciphered to "d"

For decryption 2 numbers are used. One of them is N. Second number is d (decipher exponent).

It must follow this condition:

$(d) \times (e) \pmod{\Phi(N)} = 1$

For the given example the value of d can be 4, 8, 11….

44 (mod 16) = 2 => b (decrypted message)

Advantages of RSA encryption:

- It promises confidentiality, integrity, authenticity and non-reputability of data.
- Since it's an asymmetric algorithm, managing distinct keys for every other user is avoided.
- The prime numbers of the public key are not known to anyone other than the person intended to get the message and these numbers are enormous, which makes it extremely difficult for a person or a machine to guess the prime numbers used for modulus arbitrarynumbers (produced by multiplication of the prime numbers). [15] [16]
- The brute force is not at all feasible in the case of RSA, because even the most advanced computer to ever exist till date will take up-to 1 year, if around 15 million modern computers work simultaneously. Forget about 2048, 3072 or 7680 bits RSA keys. [15][17]
- It is very easy to implement once we know the math behind it.

Limitations of RSA encryption:

- The main advantage of RSA cipher is length of key, the larger is the length of key, the longer it will take to crack the encryption but this is also making this process slower and more power consuming. If we consider mobile it's practically not appropriate to use RSA encryption for security in mobile phones because of the high computational power required along with more battery consumption.
- Different attacks can be performed against RSA:
  - Protocol failure attacks: protocol failure means these are not weaknesses of the cryptosystem, but the failure of the way it is being implemented. [16] [17] [18]
  - Common modulus attack: If a person sends the same message to more than 1 user in the network with the same common modulus N, Then the cipher text can be cracked using an extended Euclidean algorithm.
  - Low exponent attack: If a person sends the same message to 3 or more people using different public keys and chooses a low exponent to save computational time to encrypt the data, then the cipher text can be decrypted using the Chinese remainder theorem.
- Side channel attacks: these attacks involve the analysis of executiontime, electromagnetic emission, power consumption etc. [18]
- Timing attack: Timing attacks is analyzing the differences between execution times. Timing attack may give the idea of length of the input parameters along with bits of the secret RSA exponent. This is the most effective type of side channel attack on an RSA cipher.
- Other attacks: [16] [17]
- Factorization attack: If the implementation of RSA is done carelessly to save computational power and time. It may result in having a shorter length of modulus which makes it easier for an attacker to guess the prime numbers.
- Chosen cipher attack: In this attack, a cipher text is chosen and it is multiplied with a random text encrypted with the same public key and hopefully some phishing attack or reverse social engineering would work and attacker would get the decrypted message of the manipulated encrypted message. This would reveal the decryption exponent which can be used to recreate the private key.

Elliptic Curve Cryptography(ECC)

ECC stands for elliptic curve cryptography. This is asymmetric encryption which provides equal security with smaller key size as compared to other asymmetric encryption techniques (i.e. RSA). As we know, the long size key generation would take more time and computational power, that's why it's more efficient to use ECC over RSA. In this encryption technique public key and private key are generated using a mathematical cubic function. i.e. y= x3 + ax + b. [2] [19] [20]

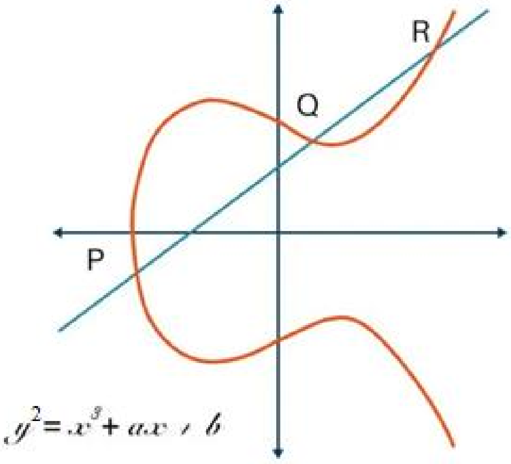


Fig 12. Elliptic curve[19]

As we can see in the given figure, a single straight line can cut the graph to a max of 3 distinct points. This graph can expand to infinity but to perform mathematical operations, we limit this graph to "n". It is symmetric to the x-axis. ECC uses trap-door functionality same as RSA. [2] [19] [20]

Steps:

Key exchange:

A point 'G' is selected whose value would lie on the curve beyond the limited curve.

Alice will have her private key NA and public key PA would be:

$PA = NA \times G$

Bob will have his private key NB and public key PB would be:

$PB = NB \times G$

In order to exchange of secret key:

Alice performs:

$K = NA \times PB \therefore PB = NB \times G$

Bob performs:

$K = NB \times PA \therefore PA = NA \times G$

Both K will be of same value, Hence exchange of secret key is done.

ECC encryption:

1. Let the message be 'M'.
2. For M, take an encoded point on the curve "PM".
3. Choose a random integer K.
4. The cipher point will be:

   $$CM = \{KG, PM+KPB\}$$

   This cipher point will be sent to Bob

ECC decryption:

Bob will multiply first coordinate of cipher point (i.e. KG) with his private key.

$KG \times NB$

Then subtract it from the 2ndcoordinate of the pair.

$= (PM+KPB) - (KG \times NB)$

$= (PM+ K (NB \times G)) - (KG \times NB) \therefore PB = NB \times G$

$= PM$

PM is the encoded point, which can be decoded again with the curve.

Advantages of ECC:

Shorter key size: The longer the key size is, the more it will take time to generate it. Not to mention more use of the computational power and other resources. A comparison of RAS key sizes with ECC key sizes for same level of security is given below. [20] [21]

Limitations of ECC:

- Hard to Implement because of the mathematical aspect of the system.
- Comparatively costly.
- Different side channel attacks like execution time, electromagnetic emission etc, are still effective against ECC. [21]

IV. CONCLUSION

Symmetric encryption utilizes a unique key that requires it to be shared to the people who need to obtain the data, whereas asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when exchanging information. Some popular algorithms for symmetric encryption are RC4, AES, DES, 3DES, and QUAD. RSA, Diffie-Hellman, ECC are some of the Asymmetric Encryption. Implementation of ECC is toughest among others because of the complicated mathematical aspect of the algorithm. Some attacks against these algorithms are Brute-force attacks, Cipher-only attacks, Known-plaintext attack, Man in the middle, side channel etc.

Key-size of an algorithm affects memory usage and power consumption along with the speed of encryption and decryption. AES is the most robust symmetric encryption algorithm, whereas ECC turns out to be a better Asymmetric algorithm than RSA. The longer key length of RSA causes RSA to be the least secure algorithm because of potential side channel attacks. DES is the only algorithm among those discussed, to be vulnerable to brute force attack. Other algorithms' longer key sizes makes it impossible to be cracked with a brute force attack.

REFERENCES

[1] Delfs, H., Knebl, H., & Knebl, H. (2002). *Introduction to cryptography* (Vol. 2). Heidelberg: Springer.

[2] Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

[3] Mollin, R. A. (2006). *An introduction to cryptography*. Chapman and Hall/CRC.

[4] Bellare, M., & Rogaway, P. (2005). Introduction to modern cryptography. *Ucsd Cse*, *207*, 207.

[5] Mahajan, P., & Sachdeva, A. (2013). A exploring ofAES, DES and RSA encryption algorithms for security. *Global Journal of Computer Science and Technology*.

[6] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19).

[7] Patil, P., Narayankar, P., Narayan, D. G., &Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617-624.

[8] Smid, M. E., & Branstad, D. K. (1988). Data encryption standard: past and future. *Proceedings of the IEEE*, *76*(5), 550-559.

[9] Penchalaiah, N., & Seshadri, R. (2010). Effective Comparison and evaluation of DES and Rijndael Algorithm (AES). *International journal of computer science and engineering*, *2*(05), 1641-1645.

[10] Courtois, N. (2005). The best differential characteristics and subtleties of the Biham-Shamir attacks on DES. *Cryptology ePrint Archive*.

[11] Akkar, M. L., & Giraud, C. (2001, May). An implementation of DES and AES, secure against some attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 309-318). Springer, Berlin, Heidelberg.

[12] Bonneau, J., & Mironov, I. (2006, October). Cache-collision timing attacks against AES. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 201-215). Springer, Berlin, Heidelberg.

[13] Selmane, N., Guilley, S., & Danger, J. L. (2008, May). Practical setup time violation attacks on AES. In *2008 Seventh European Dependable Computing Conference* (pp. 91-96). IEEE.

[14] Zhou, X., & Tang, X. (2011, August). Research and implementation of RSA algorithms for encryption and decryption. In *Proceedings of 2011 6th international forum on strategic technology* (Vol. 2, pp. 1118-1121). IEEE.

[15] Rahman, M. M., Saha, T. K., &Bhuiyan, M. A. A. (2012). Implementation of RSA algorithm for speech data encryption and decryption. *IJCSNS International Journal of Computer Science and Network Security*, *12*(3), 74-82.

[16] Boneh, D. (1999). A 20-years attack on the RSA cryptosystem. *Notices of the AMS*, *46*(2), 203-213.

[17] Nara, R., Satoh, K., Yanagisawa, M., Ohtsuki, T., & Togawa, N. (2010). Scan-based side-channel attack on his RSA cryptosystem using scan signatures. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, *93*(12), 2481-2489.

[18] Nitaj, A., Ariffin, M. R. K., Nassr, D. I., & Bahig, H. M. (2014, May). New attacks on the RSA cryptosystem. In *International conference on cryptology in Africa* (pp. 178-198). Springer, Cham.

[19] Singh, L. D., & Singh, K. M. (2015). An implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, *54*, 73-82.

[20] Alam, M., Jahan, I., Rosario, L. J., & Jerin, I. (2016). A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems. *algorithms*, *1*, 2.

DOI: 10.48175/IJARSCT-18097

[21] Amounas, F., & El Kinani, E. H. (2012). ECC encryption and decryption by data sequence. *Applied Mathematical Sciences*, *6*(101), 5039-5047.

[22] Padmavathi, B., & Kumari, S. R. (2013). A survey on performance analysis of DES, AES and RSA algorithms along with LSB substitution. *IJSR, India*, *2*, 2319-7064.

[23] Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December). An experimental study on performance evaluation of asymmetric encryption algorithms. In *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12)* (pp. 121-124).