iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.47848

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

A Study of Cryptographic Algorithms

Dr. Manjot Kaur Bhatia[1], Rajshekhar Singh Rajpurohit[2], Gulafshan[3], Benjamin Joseph[4]
[1, 2, 3, 4] *Jagan Institute of Management Studies, Rohini Sector-5*

Abstract: ***This paper explores many important Symmetric and Asymmetric Cryptography algorithms and their essence in network security. As the use of the internet has grown, so have attacks on the communication channels. These attacks can be used by third parties to obtain sensitive data about your organization and its activities. This data can be used to compromise an organization's operations or blackmail the organisation to pay for the data. To avoid these situations, such algorithms are adapted to protect communications. These algorithms encrypt data that is nearly impossible for unauthorized persons to read, making it unusable for attackers. These algorithms therefore play an important role in the security of communications.***
This paper states a study of symmetric and asymmetric algorithms in terms of optimal resource allocation, potential attacks which can be used to exploit these algorithms, time consumption, power consumption, overall structure and some other basis Along with explanation of some of the security attacks.
Keywords: CIA triad, NIST, FIPS, eavesdropping, DES, AES, RSA, ECC, Symmetric cipher, Asymmetric cipher.

I. INTRODUCTION TO CRYPTOGRAPHY

In today's world, the most precious element is data. Data can tell us a lot about an organization's strengths and weaknesses. The one who can possess and process this data with statistical and/or logical techniques can ultimately affect activities of organization actively or passively. Hence arises the question, shouldn't there be some security features for this vital element? This is where cryptography comes into play. Cryptography consists of securing information and communication with techniques derived from mathematical concepts and rule- based calculations called algorithms. The ideal cryptography technique would let decipher the data by only those for whom the information is intended.[1][2][3][4]

A. Cryptography Goals

The ultimate goal of cryptography is to secure information that can't be deciphered by third party personnel who are not supposed to receive the message. This goal may be softened into several sub-goals.[2] These are listed below

1) Confidentiality

This term covers 2 connected concepts:

a) *Data Confidentiality:* This concept assures that personal data is made available only to the authorized personnel.
b) *Privacy:* This concept makes sure that the information collected is available only to the intended receivers and not shared further.

2) Integrity

This term covers 2 connected concepts:

a) *Information Integrity:* The information is modified solely in a specified and approved way.
b) *System Integrity:* Ensures that a device/software performs its operations in a robust way, free from forced or accidental unauthorized manipulation of the system.

3) *Availability:* Ensures that systems work whenever available and repair is made available to the authorized users. The above listed objectives are known as the CIA triad. The 3 ideas embody the fundamental security objectives for informational and computational services. As an example, the NIST standard FIPS 199 (Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems) lists confidentiality, integrity, and availability because of the 3 security objectives for information and for information systems. FIPS 199 provides a helpful characterization of those 3 objectives in terms of needs and also the definition of a loss of security in every category: [3][1]

a) *Confidentiality:* Protective approved restrictions on information access and revelation, as well as suggests that for shielding personal privacy and proprietary information.
b) *Integrity:* Guarding against improper information, modification or destruction, as well as making certain information non-repudiational and believable. Unauthorized manipulation of information is loss of integrity.

©IJRASET: All Rights are Reserved

c) Availability: This is about ensuring the timely and reliable access to and use of data. A loss of availability is the disruption of access to use of data or associated systems.

Though the utilization of the central intelligence agency triad to outline security objectives is well established, some within the security field feels that extra unit required to give a whole image. Two of the foremost unremarkably mentioned area units are as follows: [1][3][4]

4) Authenticity: the property of being real and having the ability to be verified and trusted; confidence within the validity of a transmission, a message, or message conceiver. This implies that users are who they say they are and the information arrived at the system came from a trusted source.

5) Accountability: The principle of accountability refers to an entity being answerable to authority for any loss or misuse of that information. Since ideal secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to help forensic analysts trace back in case of security breach or transaction disputes.

B. How does Cryptography Work?

Let's say there are two people, Alice and Bob who want to communicate and share information about the future ambitions of their company. They are using some regular insecure channel to communicate. Because this information is crucial to the company's future operations, it must be protected. If Oscar, who is not supposed to receive this vital information, obtains it through eavesdropping tactics and wishes to thwart their objectives, he can easily do so by distorting the data by stealing their intellectual property and selling it to someone else.[2][4]

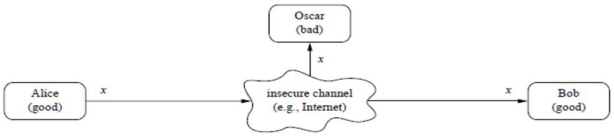


Fig 1. Communication Over an insecure Channel [2]

Cryptography can help to mitigate such hazards. The symmetric cipher (which has been modernized on a massive scale) is a rudimentary type of encryption approach in which one secret key is shared by a secured channel between Alice and Bob before communication begins. This secure route could be a face-to-face meeting or another way. This key will be used by the sender to encrypt the message and by the recipient to decrypt the data. Plain text refers to unencrypted data, while cypher text refers to encrypted data. Even if Oscar listens in on their chat, he won't be able to decipher the message because it will be encrypted using a secure key that only Alice and Bob have. As a result, all critical data will be protected, and even if someone gains access to critical messages, they will be unable to decrypt them without the private key, which will be held only by those who are supposed to receive them.[2][3]

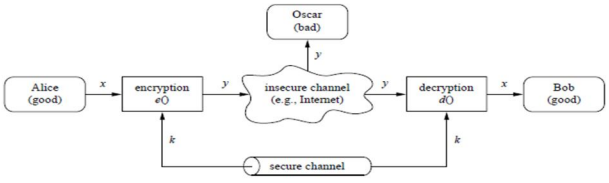


Fig 2. Symmetric-key cryptosystem [2]

- 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 vital thing to remember is that the private key must be kept secret, but the algorithm can be made public. It makes sense to keep the method confidential in order to prevent third parties from decrypting the communication, but keeping the algorithm private also indicates that it has not been tested. Making an encryption method's algorithm public and allowing other cryptographers to study it is the best way to determine whether it is strong enough or can be decoded by determined attacker. The private key is the only thing that must be kept hidden.

C. Remark

Here, the only thing under consideration is confidentiality, that is hiding the contextual meaning of the message from people with unauthorized access. Cryptography can also be used to avoid third party from making unnoticed changes in the data (message integrity) or assure the data is really coming from an authenticated user. (message authenticity)

II. TYPES OF CRYPTOGRAPHY

There are mainly two types of cryptography:-

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

A. Symmetric Cipher

The symmetric cipher makes use of only one private key to encrypt the data and this same key is used to decrypt the data. If Alice wants to send a message to Bob, she can use the K1 private key and this K1 private key will be used on Bob's side as well to decrypt that message. [2][3]

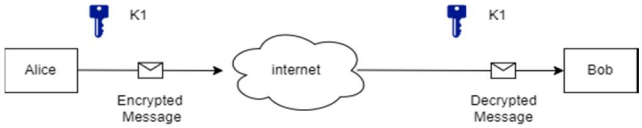


Fig 4. Symmetric encryption between 2 users[5]

Now, if a third party, say Charlie, wants to send a message to Alice, she should use a different key than K1 because K1 is already in use to establish secure communication between Alice and Bob, and both of them have this key, so even if the message is only intended for Alice, Bob can decrypt it using his key. To circumvent this, every two people on the network must communicate using a unique key.

Same thing goes for establishing a connection between Charlie and bob.

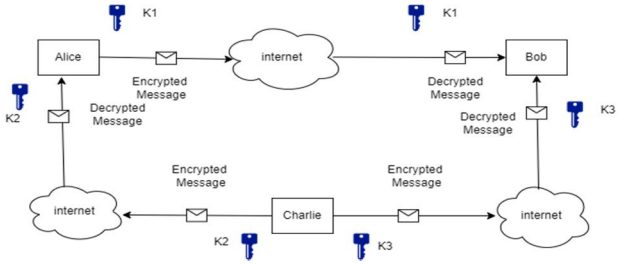


Fig 3. Symmetric encryption among more than 2 users[5]

Drawbacks

- The primary drawback of symmetric encryption is the increasing amount of unique keys required to interact with various users. If one person needs to communicate with 100 others, they must manage and keep 100 keys safe, which would make encryption a lot more hectic than it needs to be.
- Another critical disadvantage of using symmetric encryption is that the private key must be shared with both parties in order to have secured communication. Since there can't be any electronic communication which can guarantee 100% security.

B. Asymmetric Cipher

To overcome the drawback of symmetric cipher, asymmetric cipher was introduced by Whitfield Diffie and Martin Hellman in 1977. Also known as public-key cryptography.

Instead of having only one unique key, this has two. As in symmetric cypher, one is the private key. The other is the public key, which is held by all members in a network. If the data is encrypted with a public key, the data will be decrypted with a relative private key. When a private key is used to encrypt data, the associated public key is used to decrypt it. Thus, the sender is always verified.

The catch here is that the public key would encrypt the message on the basis of the recipient's private key and vice versa. If Alice wants to send a message to Bob using asymmetric encryption, she must encrypt the message using Bob's public key; however, this message can only be decoded using Bob's private key, which is only in Bob's possession. As a result, each connection does not require a unique key, but rather a single unique key for anyone on the network and a public key held by everyone. Same would happen in case of Charlie sending message to Alice or Bob.[2][3]

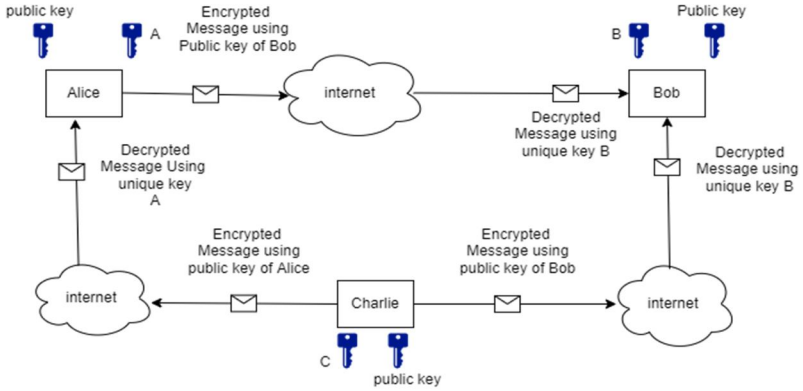


Fig 5. Asymmetric encryption[6]

1) Advantages over Symmetric Encryption

- Key distribution problem is solved.
- Since there's no need to transmit secret keys, it's more secure than symmetric encryption.
- The use of digital signatures is allowed, therefore the recipient can verify the source of the message. That is, message authenticity is achieved.
- It allows non-repudiation so that the sender can't deny sending a message.

2) Disadvantages

- It is a comparatively slow process, that's why it is not appropriate to use it for decrypting bulk messages.
- If a person lost their private key, they cannot decrypt their messages.
- If an unauthorized actor identifies someone's private key, they can interpret their messages.

III. WORKING OF ALGORITHMS

A. 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]

1) Operations on Message

a) Initial permutation: In this the 64 bit block data is handed over to an initial permutation function.
b) 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).
c) These both blocks are operated in a total of 16 rounds with a private key.
d) Final permutation is performed. This permutation is also called inverse initial permutation.

2) Operations on Key

a) Initially the key size is 64 bit.
b) 8 Parity bits (8, 16, 24, 32, 40, 48, 56, 64) are removed and the key size becomes 56 bits.
c) These 56 bits will be divided into two equal sized blocks of 28 bits each.
d) 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.

e) 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.

f) Now a permutation function will choose 48 bits from 56 bits and arrange them. It is called "Compression-Permutation operation".

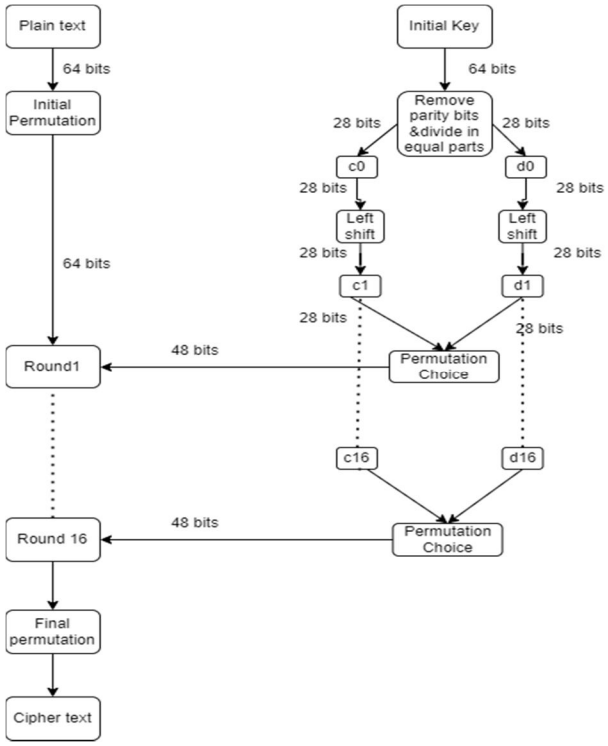


Fig 6. The layout of DES algorithm[6]

3) Core operations in Each Round

a) Left plain text (LPT) block and one copy of right plain text (RPT) will be passed at the end..

b) Right plain text block will have bits expanded by expansion permutation. (from 32 bits to 48 bits)

c) This 48 bit block will perform XOR operation with the sub-key.

d) This 48 bit resultant block will be passed with substitution blocks (s-block) and ultimately turned into 32 bits block.

e) This 32 bit block will be again permuted.

f) This processed RPT will perform XOR with LPT.

g) The copy of initial RPT will work as LPT and processed RPT will be RPT for the next round.

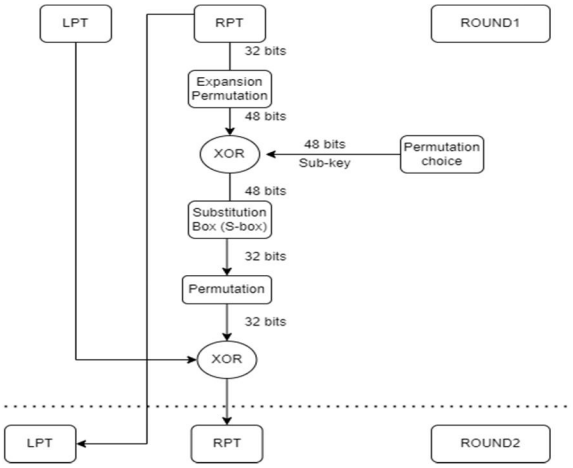


Fig 7. Internal working of DES[6]

4) Substitution box Operations: [10] [11]

a) 8 s-boxes work simultaneously to process 48 bits data blocks.

b) 6 bits are passed to each s-box.

c) 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.

d) Whatever data on that specific position in the initial 64 bit data table will be converted to 4 bits binary form.

e) Bits of this binary number will be output of s-box.

f) Every s-box will convert 6 bits into 4 bits. Hence 48 bits into 32 bits.

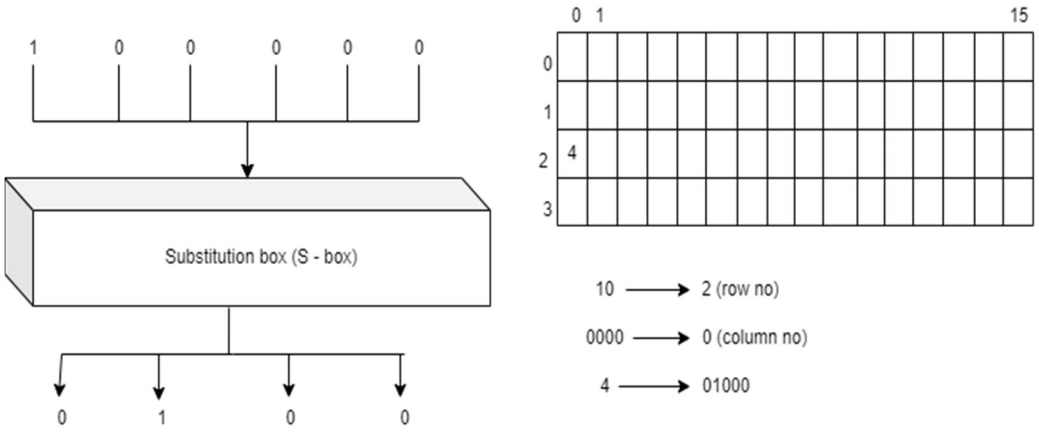


Fig 8. S-box illustration [10]

DES Limitations

- *Key Size:* The sub-key is only of size 56 which results in 2^{56} 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 2^{56} 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]

C. Advanced Encryption Standards (AES)

AES stands for advanced encryption standards.

1) Operation on Message: [9][11][12]

a) Whole message is divided into blocks of 128 bits.

b) This 128 bits block would be in the form of a 4x4 matrix whose one cell would have size of 1byte (8bits).

c) The block would be performing XOR operation with k0 sub-key and generate a state matrix. (intermediate form)

2) AES Transformation Function

a) 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]

b) 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]

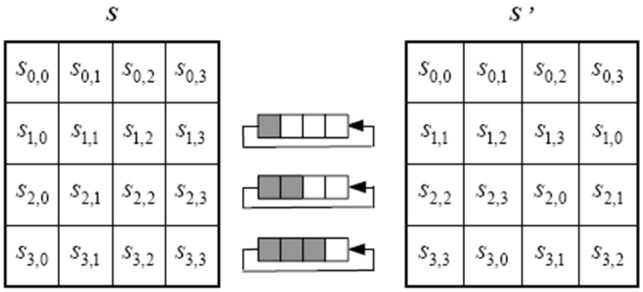


Fig 10. Row shift step[13]

c) 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]

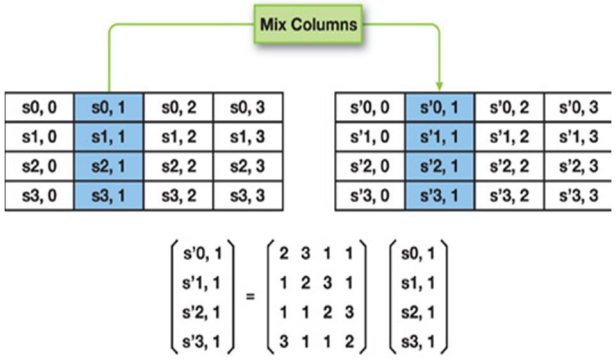


Fig 11. Mix column[13]

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

3) Operations on key

a) 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.

b) Key generator function is used to generate subkeys.

c) 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.

D. 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]

1) Steps for RSA Encryption

a) Two random prime numbers are generated.

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

b) 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

c) Φ(N) is calculated. (Φ(N) gives the number of co-prime numbers with N, from 1 to N).

Φ(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.

d) 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 Φ(N) and It must be coprime with N and Φ(N).

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

In this case the number is 5.

e) 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 => $2^5 \pmod{16} = 4$

4^{th} index alphabet = "d"

So "b" is ciphered to "d"

f) 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….

$4^4 \pmod{16} = 2$ => b (decrypted message)

2) Advantages of RSA encryption

a) It promises confidentiality, integrity, authenticity and non-reputability of data.

b) Since it's an asymmetric algorithm, managing distinct keys for every other user is avoided.

c) 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 arbitrary numbers (produced by multiplication of the prime numbers). [15] [16]

d) 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]

e) It is very easy to implement once we know the math behind it.

3) Limitations of RSA Encryption

a) 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.

b) 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 execution time, 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.

E. 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. $y = x^3 + ax + b$. [2] [19] [20]

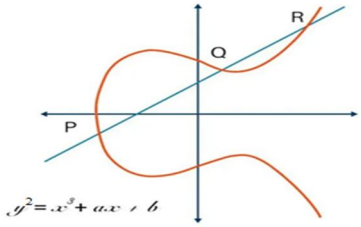


Fig 12. Elliptic curve[19]

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

1) *Key Exchange*
   a) A point 'G' is selected whose value would lie on the curve beyond the limited curve.
   b) Alice will have her private key N_A and public key P_A would be:

$$P_A = N_A \times G$$

   c) Bob will have his private key N_B and public key P_B would be:

$$P_B = N_B \times G$$

   d) In order to exchange of secret key:
      i) Alice performs:

$$K = N_A \times P_B \qquad \therefore P_B = N_B \times G$$

      ii) Bob performs:

$$K = N_B \times P_A \qquad \therefore P_A = N_A \times G$$

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

2) *ECC Encryption*
   a) Let the message be 'M'.
   b) For M, take an encoded point on the curve "P_M".
   c) Choose a random integer K.
   d) The cipher point will be:

$$C_M = \{KG, P_M + KP_B\}$$

   e) This cipher point will be sent to Bob

3) *ECC Decryption*
   a) Bob will multiply first coordinate of cipher point (i.e. KG) with his private key.

$$KG \times N_B$$

   b) Then subtract it from the 2nd coordinate of the pair.

$$= (P_M + KP_B) - (KG \times N_B)$$
$$= (P_M + K(N_B \times G)) - (KG \times N_B) \qquad \therefore P_B = N_B \times G$$
$$= P_M$$

   c) P_M 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]

RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

Fig 13. Key size comparison[19]

- Elliptic curve integrated encryption schemes (ECIES): ECC algorithm can be used to share secret keys along with encryption of data. It is a comparatively more secure way to exchange secret keys.

➢ *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. COMPARATIVE ANALYSIS

One cannot conclude if symmetric algorithms are better or asymmetric, since one may be better in some aspects but at the same time it can also lack some other aspects. And the fact that there are different variations of the same algorithms can make it more complicated to find out the best one. Algorithms can be preferred according to the needs. [22] [23]
Differences between different types of symmetric and asymmetric algorithms of cryptography on some classical parameters are as follows:

Parameters	AES	DES	RSA	ECC
Key Size (bits)	128, 192, 256	56	>1024	>160
Type	Symmetric	Symmetric	Asymmetric	Asymmetric
Encryption speed	Fast	Moderate	Slower	Fast
Decryption speed	Fast	Moderate	Slower	Fast
Power Consumption	Low	Moderate	High	Moderate
Memory Usage	Moderate	Low	Moderate	Low
Security	Most secure	Less secure	Least secure	Secure
Attacks	Side channel attacks	Brute-Force attack, Differential cryptanalysis, Linear cryptanalysis, Davies attack	Protocol failure attacks, side channel attacks, Factorization attack, chosen cipher attack	Pohlig-hellman attack, pollard's rho attack

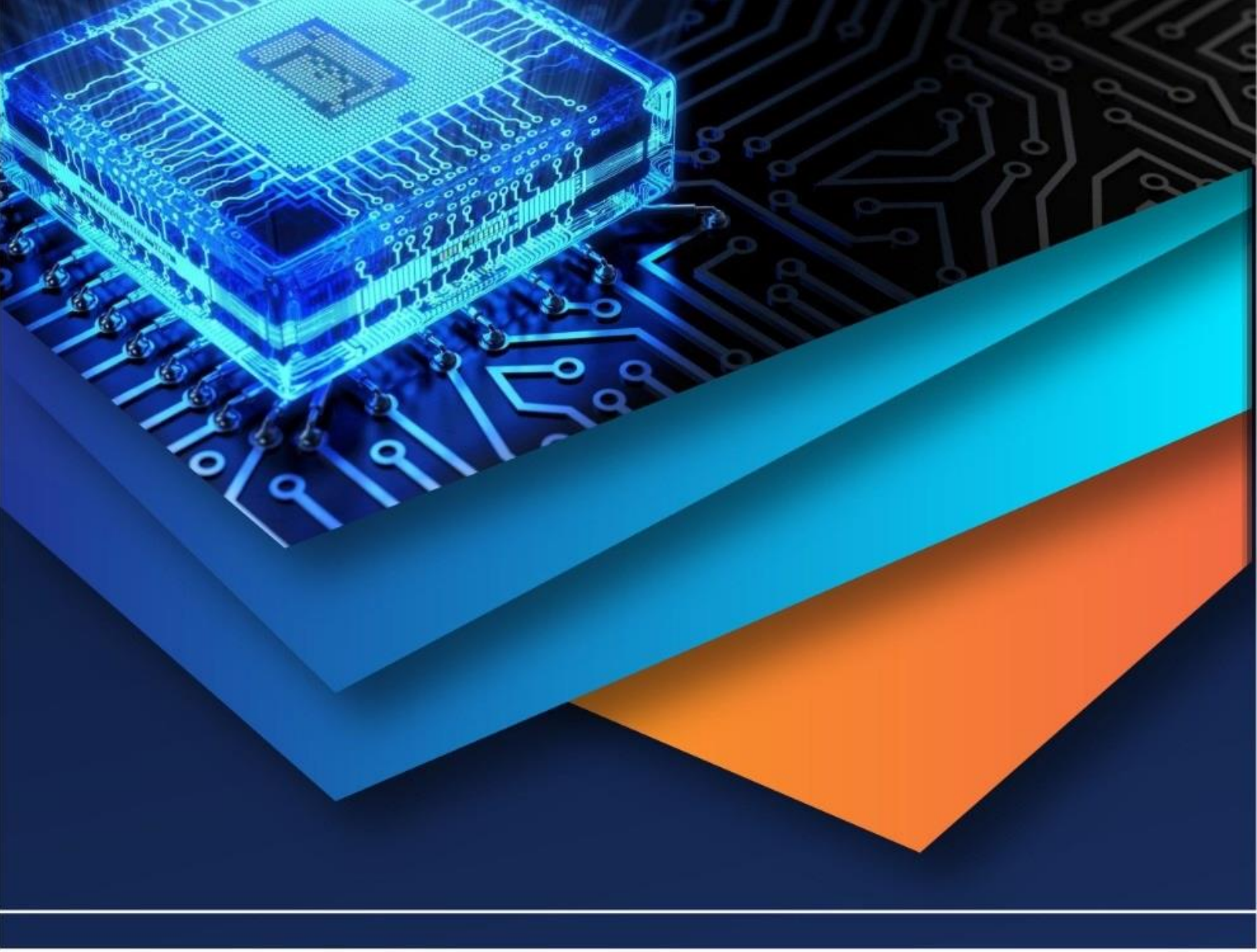
V. CONCLUSION

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 of AES, 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.
[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).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)