A Survey on Various Encryption Techniques

M.Prabhavathy[1], Meenakshi Sundharam[2], M.S Ramesh[3], Bubesh .P[4], HaswinRaj.V[5]
[1]Assistant Professor, Dept of CSE
[2, 3, 4, 5] Dept of CSE
[1, 2, 3, 4, 5] Coimbatore Institute of Technology

Abstract- *This paper will present a perspective on the various encryption algorithms, in particular on private key block ciphers which are widely used for bulk data and link encryption. We have initially survey some of the more popular and interesting algorithms currently in use .This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey.This paper sheds light on the pros and cons each encryption algorithm holds and also the particular scenarios in which they can be applied to and the security level they bring into the system.*

I. INTRODUCTION

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher-text that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues.

1.1 Basic Terms Used in Cryptography

- **Encryption:**

Process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things-an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

- **Decryption:**

Reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things-a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same

- **Key :**

Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it.

- **Plain Text:**

The original message that the person want to communicate is defined as plain text. For an example, Alice is a person wishes to send “Hai, How are you” message to person Bob, “Hi friend how are u “is referred as plain text.

- **Cipher Text**:

The message which cannot be understood by anyone is defined as cipher text for an example “ ib%ipvbufzpv@ “ is a cipher text produced for plain text “Hi , How are you “.

- **Access Control:**

Access Control (AC) is the selective restriction of access to a place or other resource while access management describes the process. Access control decisions are made by comparing the credentials to an access control list. This look-up can be done by a host or server, by an access control panel, or by a reader.

- **Authorization:**

Authorization is the function of specifying access rights/privileges to resources.During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected).

- **Symmetric Encryption:**

Symmetric encryption involves only one secret key to cipher and decipher information. Symmetrical encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption.

- **Asymmetric Encryption:**

Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.Popular asymmetric key encryption algorithm includes RSA, DSA, Elliptic curve techniques.

- **Digital Certificates:**

A certificate is a package of information that identifies a user and a server. It contains information such as an organization's name, the organization that issued the certificate and users public key. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

- **Public Key:**

In asymmetric encryption, two keys are used in which one is transmitted public and it is used to encrypt the message that is transferred between the communicating parties. This key may not be needed for decryption purposes as the private key is used here but based on various algorithms, some may need to use the public key for decryption.

- **Private Key:**

These keys are always needed to be kept secret by the holding parties to ensure security of the messages transferred else there is a security breach. In asymmetric encryption, these keys are used to decrypt the messages encrypted by public keys.

- **Digital Signatures:**

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.They provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender.Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message.

1.2 Classification of Cryptography

Encryption algorithms can be classified into two broad categories-Symmetric and Asymmetric key encryption.

- **Symmetric Encryption:**

In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc.

- **Asymmetric Encryption:**

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

II. CRYPTOGRAPHIC ALGORITHMS

- **DES :**

Data Encryption standard(DES)[1]mainly adopted by industry for security products. Algorithm design for

encryption and decryption process has been done with same key. This algorithm processes the following steps.

1. DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
3. The plaintext and key will processed by following
   a. Key is split into two 28 halves.
   b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
   d. The rotated key halves from step 2 are used in next round.
   e. The data block is split into two 32-bit halves.
   f. One half is subject to an expansion permutation to increase its size to 48 bits.
   g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
   h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   i. Output of step 8 is subject to a P-box to permute the bits.
   j. The output from the P-box is exclusive-OR'ed with other half of the data block.
   k. The two data halves are swapped and become the next round's input.

Advantages:

1. It's a 56 bit key. So there are 2^56 possibilities of keys which would take a decade to find the correct key using brute-force attack
2. Encryption and decryption takes the same algorithm. Only that the function need to be reversed and the key should be taken in opposite order. This is very convenient for software and hardware requirements.

Disadvantages:

1. Weak keys : the key that is selected on the rounds are a problem . During splitting of keys to two half and swapping them might throw up the same result if they have continuous 1's and 0's. Thins ends up in using the same key through out the 16-cycles
2. There can be same output from the S-Boxes on different inputs on permutation. These are called Semi weak keys.
3. If the message is encrypted with a particular key, and is taken 1's compliment of that encryption will be same as that of the encryption of the compliment message and compliment key.

- **AES :**

Advanced Encryption Standard (AES)[1] algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10,12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

The following steps processed in AES algorithm Following steps used to encrypt a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation. Perform the tenth and final round of state manipulation.
5. .Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations .

They are ,

a. **Sub Bytes** : This operation is a simple substitution that converts every bite into a different value.

b. **Shift Rows** : Each row is rotated to the right by a certain number of bytes.

c. **Mix Columns** : Each column of the state array is processed separately to produce a new column. The new column replaces the old one.

d. **Xor Round Key** :This operation simply takes the existing state array, Decryption: Decryption involves reversing all the steps .

Advantages:

- As it is implemented in both hardware and software, it is most robust security protocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.
- It is most common security protocol used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
- It is one of the most spread commercial and open source solutions used all over the world.
- No one can hack your personal information.
- For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

Disadvantages:

- It uses too simple algebraic structure.
- Every block is always encrypted in the same way.
- Hard to implement with software.
- AES in counter mode is complex to implement in software taking both performance and security into considerations

- **RSA :**

Rivest Shamir Aldeman is the most commonly used public key encryption algorithm. RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider[2].

RSA is too slow for encrypting large volumes of data .but it is widely used for key distribution.

Following steps are followed in RSA to generate the public and private keys

1. Conisder two large prime numbers p and q such that p~=q.
2. Compute n=p*q
3. Compute φ (pq) = (p-1)*(q-1)
4. Consider the public key k1 such that gcd (φ (n), k1) =1; 1<k1< φ (n)
5. Select the private key k2 such that k2*k mod φ (n) =1

Encryption and Decryption are done as follow

Encryption : Calculate cipher text C from plaintext P such that C=P ^k1 mod n

Decryption : P=C^k2 mod n=P^k1k2 mod n.

Advantages:

The advantages include

- RSA algorithm is safe and secure for its users through the use of complex mathematics.
- RSA algorithm is hard to crack since it involves factorization of prime numbers which are difficult to factorize.
- Moreover, RSA algorithm uses the public key to encrypt data and the key is known to everyone, therefore, it is easy to share the public key.

Disadvantages:

The disadvantages include

- RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer.
- It requires a third party to verify the reliability of public keys.
- Data transferred through RSA algorithm could be compromised through middlemen who might temper with the public key system.

- **Homomorphic encryption:**

Homomorphic encryption is a form of encryption that allows computation on cipher-texts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

Homomorphic encryption [3] can be used for privacy-preserving outsourced storage and computation. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted.

In highly regulated industries, such as health care, homomorphic encryption can be used to enable new services by removing privacy barriers inhibiting data sharing. For example, predictive analytics in health care can be hard to apply due to medical data privacy concerns, but if the predictive analytics service provider can operate on encrypted data instead, these privacy concerns are diminished.

Fully Homomorphic Encryption

A cryptosystem that supports arbitrary computation on cipher-texts is known as fully homomorphic encryption (FHE)[4]. Such a scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result. Since such a program need never decrypt its inputs, it can be run by an untrusted party without revealing its inputs and internal state. Fully homomorphic cryptosystems have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing.

Advantages:

- The advantage is that company A can perform computations on company B's private data without learning B's secrets.
- B might want to do this if A can perform the computations cheaper or faster than B or if A has a secret algorithm.
- It might also make sense if B has lots of other code running in A's cloud platform.
- One other advantage is that the data can be decrypted less often, which is good for security.

Disadvantages:

The downsides are

- It is extremely slow as it needs to work on large cipher texts.
- It is computationally expensive as it requires complex operations
- It is not currently practical due to working principle limitations.

- **ECC:**

ECC stands for **Elliptic Curve Cryptography**[5] is the latest encryption method offers stronger security.Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. If we compare to the RSA and DSA algorithms, then 256-bit ECC is equal to 3072-bit RSA key. The reason behind keeping short key is the use of less computational power, fast and secure connection, ideal for Smartphone and tablet too.To use ECC, all parties must agree on all the elements defining the elliptic curve, that is, the domain parameters of the scheme.

The domain parameters include,

- The prime p that specifies the size of the finite field.
- The coefficients a and b of the elliptic curve equation.
- The base point G that generates our subgroup.
- The order n of the subgroup.
- The cofactor h of the subgroup.

In conclusion, the domain parameters for our algorithms are the sextuple (p,a,b,G,n,h) .

Advantages:

- It has smaller keys, cipher texts and signatures, thus providing faster transmission speeds.
- Binary curves used are very fast in hardware.
- Signatures can be computed in two stages, allowing latency much lower than inverse throughput.
- The key generation is very fast compared to all the other algorithms.
- Moderately fast encryption and Decryption.

Disadvantages:

- Complicated and tricky to implement securely, particularly the standard curves.
- Standards aren't state-of-the-art, particularly ECDSA
- Signing with a broken random number generator compromises the key.
- Newer algorithms could theoretically have unknown weaknesses.
- Difficult to understand and implement.

- **DSA:**

DSA stands for Digital Signature Algorithm.DSA[6] is one of the many algorithms that are used to create digital signatures for data transmission.In DSA, a pair of numbers is created and used as a digital signature. These are generated using some specific algorithms.DSA is used only to create the signatures. They cannot be used for encryption of data.

Unlike mutual key exchange algorithms like RSA the digital signature algorithm does not use a private key to encrypt data. Also, a digital signature algorithm does use a public key to decrypt this data. To create a digital signature with two 160-bit numbers, DSA works on the principle of a unique mathematical function. These two numbers are made by using the private key and the message digest which is created using a hash function.

Advantages:

- Along with having strong strength levels, the length of the signature is smaller as compared to other digital signature standards.
- The signature computation speed is less.
- DSA requires less storage to work as compared to other digital standards.
- DSA is patent free so it can be used free of cost.

Disadvantages:

- It requires a lot of time to authenticate as the verification process includes complicated remainder operators. It requires a lot of time for computation.
- Data in DSA is not encrypted.We can only authenticate data in this.
- The digital signature algorithm firstly computes with SHA1 hash and signs it.
- Any drawbacks in cryptographic security of SHA1 are reflected in DSA because implicitly of DSA is dependent on it.
- With applications in both secret and non-secret communications, DSA is of the US National Standard.

- **Rivest Cipher (RC2) :**

RC2 (also known as ARC2) is a symmetric-key block cipher designed by Ron Rivest in 1987.RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy unbalanced Feistel network, with 16 rounds of one type (MIXING) punctuated by two rounds of another type (MASHING). A MIXING round consists of four applications of the MIX transformation followed by mashing process.

Advantages:

- Since it involves mixing and mashing of the blocks of input data, it is easy to implement.
- The block size is 8 bytes which is sufficiently larger than other block cipher systems in practice.
- Since the input data is broken into blocks, it is easier to access them during both the encryption and the decryption phases.

Disadvantages:

- RC2 is vulnerable to a related-key attack using 2^{34} chosen plaintexts.
- If the attacker happens to observe the operation of cipher under several different keys they could easily decrypt the messages.
- If some mathematical relationship connecting the keys is known to the attacker then the whole purpose of encryption fails.

- **Blowfish(cipher)**

Blowfish is a symmetric-keyblock cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software. Blowfish is an open-source algorithm which was first proposed as an alternative to aging DES algorithm .Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits It is a 16-round Feistelcipher[8] and uses large key-dependent S-boxes[7].

Advantages:

- Blowfish is a fast block cipher, except when changing keys.
- Blowfish has a memory footprint of just over 4 kilobytes of RAM.
- Blowfish was one of the first secure block ciphers not subject to any patents and therefore freely available for anyone to use.
- The extra computational effort required gives protection against dictionary attacks.

Disadvantages:

- Blowfish's use of a 64-bit block sizemakes it vulnerable to birthday attacks, particularly in contexts like HTTPS.
- A reduced-round variant of Blowfish is known to be susceptible to known-plaintext attacks on reflectively weak keys.
- Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers.
- Due to 4kb of RAM requirement it does prevent use in the smallest embedded systems such as early smartcards.

III. CONCLUSION

The paper has summarized the various encryption techniques that are currently in use across the internet. Many of these cryptographic algorithms find their usage in various applications. With the advent of IOT, security for data is at a

level of importance more than any other things. Thus one can refer to this comparative study and choose specific algorithm for their application that suits their purpose. This survey of various encryption techniques compared algorithms across various types starting from symmetric to asymmetric encryption types to block encryption. Thus we hope this paper will provide the reader with enough knowledge to determine the algorithm that they need to improve the security for their application and hence serve the purpose.

REFERENCES

[1] BawnaBhat ; Abdul Wahid Ali ; Apurva Gupta , "DES and AES performance evaluation",International Conference on Computing, Communication & Automation (2015).
[2] KannanBalasubramanian , "Variants of RSA and their cryptanalysis", 2014 International Conference on Communication and Network Technologies (2014).
[3] Dalia Tourky ; Mohamed ElKawkagy ; ArabiKeshk , "Homomorphic encryption the "Holy Grail" of cryptography" , 2016 2nd IEEE International Conference on Computer and Communications (2016).
[4] Konstantin G. Kogos ;Kseniia S. Filippova ; Anna V. Epishkina , "Fullyhomomorphic encryption schemes: The state of the art", 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (2017).
[5] XianjinFang ;Yanting Wu, "Investigation into the elliptic curve cryptography" , 2017 3rd International Conference on Information Management (ICIM) (2017).
[6] DhananjayaSingh ; Parma Nand ; Rani Astya ; Payal Dixit , "Improved DSA cryptographic protocol and its comparative study with RSA protocol",International Conference on Computing,Communication & Automation (2015).
[7] TingyuanNie ;Teng Zhang , "A study of DES and Blowfish encryption algorithm" , TENCON 2009 - 2009 IEEE Region 10 Conference (2009) .
[8] Chun Guo , "Understanding the Related-Key Security ofFeistel Ciphers" , IEEE Transactions on Information Theory (2019) .