A Review on Cryptography and Cryptography Techniques

Smt. Sneha S. Gholap
HoD, Department of Mathematics
MVP Samaj's, GMD Arts,BW Commerce
and Science College, Sinnar.
Dist.- Nashik 422103(MS) India.

Dr. Dhanashri A. Munot
Department of Mathematics
SAJVPM'S Smt. S. K. Gandhi Arts,
Amolak Science and P. H. Gandhi
Commerce College, Kada.414202

Abstract:

In today's online world, securing our information is very important. Cryptography is a technique in which the information is first encoded and then decoded so that only the intended person can read it. Information is first encoded, called as encryption, in which data is transformed into an unreadable form, and after that it is decoded, called as decryption, in which data is again transformed into a readable form. With the help of the key, this encryption and decryption are done. Based on key distribution, cryptography is categorised mainly into two important types: Symmetric key cryptography and Asymmetric key cryptography. In this paper, various cryptography techniques used are discussed.

Keywords: *cryptography, encryption, decryption, DES, AES, blowfish, digital signature.*

Introduction:

For every person, protecting personal and sensitive information is very important. Use of online platforms is increasing day by day. More aspects of our daily lives including communication, financial transactions, military, and healthcare services are conducted online. Cryptography plays an important role in protecting the data. It involves encryption and decryption of the messages. Encryption is the process of converting a plane text into ciphertext, and decryption is the process of getting back the original message from the encrypted text. It prevents unauthorised access to the information. For this, many encryption techniques exist that are used to avoid information theft. The purpose of cryptography is confidentiality, authentication, integrity, non-repudiation, access control and availability [1].

Mainly, there are two encryption techniques: Symmetric key cryptography and Asymmetric key cryptography.

1) Symmetric key cryptography: In symmetric key cryptography, both parties utilise the same key. With the key and encryption method sender encrypts the data, and the receiver decrypts the data with the same key and matching decryption algorithm.

2) Asymmetric key cryptography: It is also called as public key cryptography. Two keys are used in asymmetric key cryptography: a private key and a public key. The public key is used to encrypt the plaintext and only the authorised person can be able to decrypt the ciphertext through the private key. The private key is kept secret. This method is more convenient and provides better authentication, as the privacy remains intact.

- **Types of Symmetric key cryptography:**

1) DES (Data Encryption Standard): It was first developed by IBM in early 1970 and was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. It is a block cipher. It processes 64-bit blocks at a time, and the key size is also 64-bit, with 56 bits actually used by the algorithm and the remaining 8 bits serving as parity bits. Data is processed for 16 rounds. [5]

Advantages:

i) The DES algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications.

ii) Although introduced in 1976, it has proved resistant to all forms of cryptanalysis. [2]

Disadvantages

i) Its key size is too small by current standards, and the entire 56-bit key space can be searched in approximately 22 hours.

ii) It was recognised that DES was not secure because of the advancement in computer processing power.[2]

2) TDES (Triple DES or 3DES): 3DES was suggested by IBM (International Business Machines Corporation) in 1998. A substitute for DES, 3DES offers an improved key size and applies the DES algorithm three times in each data block. The key length for the 3DES is 112 and 168 bits, the number of rounds is 48, and the block length is 64 bits [2]. This algorithm aims to increase protection and security through its longer key size relative to DES. However, it is more time-consuming than DES when applied to the encryption process. [6]

Advantages

i) It uses a 64-bit block size with a 192-bit key size. It is similar to DES because the encryption method is based on the original DES, but applied three times to increase the encryption level and the average safe time.

ii) 3DES is easy to implement (and accelerate) in both hardware and software.

Disadvantages

i) 3DES is slower than other block cipher methods.

ii) It has poor performance.[2]

3) AES (Advanced Encryption Standard): AES was deployed by the National Institute of Standards and Technology in 2001; it is also called “Rijndael” [9]. AES is a block cipher with a block size of 128 bits. The key length can be 128, 192, or 256 bits. Encipherment involves ten rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The algorithm is called AES-128, AES-192, or AES-256, depending on the key size [9]. The steps for each round include four layers: substitution byte, shift rows, mix columns, and add round key[8].

Advantages

i) The purpose of the AES algorithm is to replace older and less reliable algorithms, such as the Data Encryption Standard (DES).

ii) AES encryption is fast and flexible.

iii) AES has also been employed in other areas, such as securing information on smart cards and during online transactions.

iv) Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations.

v) In June 2003, the U.S. Government announced that AES could be used to protect classified information.

vi) The design and strength of all key lengths of the AES algorithm (i.e., 128, 192, and 256 bits) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require the use of either the 192-bit or 256-bit key lengths. [2]

Disadvantages

i) Implementing AES in Galois/Counter Mode (GCM) is challenging in software.

ii) The large key size can sometimes make it complex.

4)Blowfish: Blowfish is a type of symmetric block cipher generated by B. Schneier in 1993. Blowfish is a fast algorithm, license-free, and unpatented. It uses a key length in the range of 32– 448 and a sixty-four-bit block. The Blowfish algorithm makes use 16 rounds for the encipherment procedure. Blowfish ordinarily makes use of 4 S-boxes rather than one S-box. It requires additional processing time because it relies on key length; however it provides strong safety [10].

Advantages

i) Blowfish is a very fast encryption algorithm, especially for software implementations on 32-bit microprocessors.

ii) It supports variable-length keys from 32 to 448 bits, allowing for flexible security levels.

iii)The algorithm is not patented and is free for anyone to use, which has contributed to its popularity.

iv)It has a good security record, being resistant to many cryptanalytic techniques.

v) The algorithm is relatively simple to understand and implement.

vi)It is compatible with a wide range of platforms and programming languages.

Disadvantages

i)The 64-bit block size is considered small by modern standards and can be a risk when encrypting large amounts of data with the same key (around 30 GB).

ii)The initial setup process, which includes a key schedule, is slow. This is a significant disadvantage when the key needs to change frequently.

iii) Blowfish does not provide built-in data integrity or authentication mechanisms, which means it has to be paired with other protocols for these functions.

iv) Due to the small block size, a single key should not be used to encrypt more than about 30 GB of data, as it becomes more vulnerable to certain attacks.

5) HiSea (Hybrid Cubes Encryption Algorithm): Hybrid Cube Encryption Algorithm (HiSea) is a symmetric non-binary block cipher because the encryption and decryption key, plaintext, ciphertext and internal op

eration in the encryption or decryption process that is based on integer numbers. HiSea encryption algorithm was developed by Sapiee Jamel in 2011. The plaintext size for the encryption process is 64 decimal ASCII characters of 64 bytes. The Hybrid Cube (HC) is generated based on the inner matrix multiplication of the layers between the two Magic Cubes (MC) [11].

TABLE 1: COMPARATIVE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS[7]

Algorithms/ Parameters	**DES**	**3DES**	**AES**	**Blowfish**	**HiSea**
Published	1977	1998	2001	1993	2011
Developed by	IBM	IBM	Vincent Rijmen, Joan Daeman	Bruce Schneier	Sapiee Jamel
Algorithm Structure	Feistel	Feistel	Substitution-Permutation	Feistel	Substitution-Permutation
Block cipher	Binary	Binary	Binary	Binary	Non-Binary
Key Length	56 bits	112 bits, 168 bits	128 bits, 192 bits and 256	32 – 448 bits	1 – 4096 set of integers
Flexibility or Modification	No	YES, Extended from 56 to 168 bits	YES, 256 key size is a multiple of 64	YES, 64-448 key size in multiples of 32	No
Number of Rounds	16	48	10, 12, 14	16	4
Block size	64 bits	64 bits	128 bits	64 bits	64 characters
Throughput	Lower than AES	Lower than DES	Lower than Blowfish	High	Lower than AES
Level of Security	Adequate security	Adequate security	Excellent security	Excellent security	Highly secure
Encryption Speed	slow	Very slow	Fast	Fast	Moderate
Effectiveness	Slow in both software and hardware	Slow in software	Effective in both software and hardware	Efficient in software	Efficient in software
Attacks	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack	Not yet

- **Types of Asymmetric Key Cryptography:**

1) RSA: RSA is a public key algorithm invented by Rivest, Shamir, and Adleman [7]. The key used for encryption differs from (but is related to) the key used for decryption. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key [2]. The keys for the RSA algorithm are generated in the following way:

i) Choose two distinct large prime numbers p and q.

ii) For security purposes, p and q should be chosen randomly and be of similar bit-length. Prime integers can be efficiently found using a primality test.

iii) Compute n = pq; n is used as the modulus for both the public and private keys.

iv) Select the public key (i.e., the encryption key) E such that it is not a factor of (p − 1) or (q − 1).

v) Select the private key (i.e., the decryption key) D such that the following equation holds:
(D * E) mod ((p - 1) * (q - 1)) = 1.

vi) For encryption, calculate the ciphertext CT from the plaintext PT as follows:
CT = PT^E mod N.

vii) Send CT as the ciphertext to the receiver.

viii) For decryption, calculate the plaintext PT from the ciphertext CT as follows:
PT = CT^D mod N.

Advantages:

i) As it's a stream cipher, it makes processing faster.

ii) A particular RC4 key can be used only once.

iii) Stream ciphers are immune to noise.

iv) Applicable to data whose length is either unknown or continuous.

Disadvantages:

i). Encryption/decryption time is directly related to key length and data size; as the size increases, speed decreases.

ii) One in every 256 keys can be a weak key, identified by cryptanalysis, which finds circumstances where one or more generated bytes are strongly correlated with a few bytes of the key.

iii) Stream ciphers provide no integrity protection or authentication.

2) Diffie-Hellman: This scheme was first published by Whitfield Diffie and Martin Hellman in 1976. It is a non-authenticated key agreement protocol and is used to provide forward secrecy in transport layer. In 2002, it was named as Diffie-Hellman-Merkle key exchange in recognition of Ralph Merkle's contribution to the invention of public key cryptography. This scheme uses random values to generate the key[6,15] which uses key exchange method for the same.[5]

Advantages:

1. As key is generated by key exchange method, so increases security.
2. Random values are used in key generation process.

Disadvantages:

1. If large random numbers are used, speed becomes slow because of complex calculations.
2. Susceptible to Logjam attack which allows a man in the middle attacker to read and modify any data passed over the connection.

3) ECC (**Elliptic Curve Cryptography**): The use of elliptic curves was suggested by Neal Koblitz and Victor S. Miller in 1985 and this scheme was entered as an algorithm on 2005 to 2006. It is a public key cryptography in which two keys *i.e.,* one public and one private keys are used. Public key is used to encrypt the data and private key is used to decrypt the data which increases the security level. Here random numbers are used to generate the keys[7, 24]. This scheme is so called, because by representing data bits on elliptic curve, points are obtained which are used in generation of ciphers.[5]

Advantages:

1. More secure due to public key usage.
2. It uses smaller keys to provide high speed and security.
3. Due to small key size, it reduces the storage and transmission requirements.

Disadvantages:

Complicated and tricky to implement securely, particularly the standard curves as randon numbers are used to select the curve.

4) Digital Signature: A digital signature is an electronic counterpart of a written signature that may be used to prove to the receiver or a third party that the communication was signed by the sender in reality. For stored data and programs, digital signatures may be created so that the data and programs' integrity can be confirmed at any time. The “Hash function,” which is utilized in this technique and produces dynamic and lower sizes of bits based on each byte of data, is one way for transmitting low size and capacity data using DSA. Bitwise or and multiply functions are the most common hashing functions. If the hashed file is 4 percent the size of the original file in messages less than 1600 bytes. This method may be utilized in a variety of applications that need simple and quick procedures for creating digital signatures and have a small file size for transmitting (23,24).[12]

Advantages:

i) It is very fast and provides non-repudiation and authenticity

ii) It secures the data against various attacks like Man-in-the-Middle attacks and is more advantageous than other asymmetric key algorithm.

Disadvantages:

Digital signatures have short life span.They are not compatible with each other and thus complicate sharing.[5]

TABLE 2: COMPARATIVE ANALYSIS OF ASYMMETRIC ENCRYPTION ALGORITHMS

Feature / Algorithm	RSA	Diffie-Hellman (DH)	Elliptic Curve Cryptography (ECC)	Digital Signature
Type	Asymmetric	Key Exchange	Asymmetric	Authentication/Integrity
Main Purpose	Encryption, Digital Signature	Secure key exchange	Encryption, Digital Signature	Message authentication
Key Size (for 128-bit security)	3072 bits	3072 bits	256 bits	Depends on underlying algorithm
Mathematical Basis	Integer factorization	Discrete logarithm problem	Elliptic curve discrete logarithm	Based on RSA or ECC typically
Efficiency	Slower than ECC at large keys	Moderate	High (especially for mobile/IoT)	Depends on algorithm used
Security Level	Strong, but weaker per bit	Strong, but requires large keys	Strong, higher per-bit security	Strong if underlying crypto is
Key Exchange	Supported	Primary function	Supported	Not used for key exchange
Encryption	Supported	Not supported	Supported	Not for encryption
Digital Signature Support	Supported (RSA signatures)	Not directly	Supported (ECDSA)	Main function
Performance (CPU/Memory)	High usage	Moderate usage	Low usage	Varies with the scheme
Common Variants	RSA-OAEP, RSA-PSS	DH, ECDH	ECDSA, EdDSA	RSA Signatures, ECDSA, EdDSA
Post-Quantum Security	Not secure	Not secure	Not secure	Not secure

Conclusion:

Cryptography plays a vital role in achieving the main security goals, such as authentication, integrity, confidentiality, and non-repudiation. Cryptographic algorithms are developed to accomplish these aims. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. In this paper, we review some of the research conducted in the field of cryptography, as well as how various algorithms used for different security purposes function. Cryptography will continue to evolve alongside IT and business strategies to protect personal, financial, medical, and e-commerce data and to ensure a respectable level of privacy.

References:

1] Jitendra Singh Laser, Viny Jain.'A Comparative survey of various cryptography techniques', International Research Journal of Engineering and Technology(IRJET), volume: 03, issue: 03, March 2016

2] Mitali, Vijay Kumar and Arvind Sharma.'A survey on various cryptography techniques', International Journal of Emerging Trends and Technology in Computer Science (IJETTCS),2014

3] Agrawal T, Agrawal Ak, Singh Sk.'An efficient key-accumulation cryptosystem for cloud', International Journal of Engineering Advanced Technology,2019.

4] Bharati Kaushik, Vikas Malik, Vinod Saroha.'A review paper on data encryption and decryption', International Journal for Research in Applied science and Engineering Technology (IJRASET), April 2023.

5] Neha Tayal, Ritesh Bansal, Shailender Gupta and Sangeeta Dhall. 'Analysis of Various Cryptography Techniques: A survey'.International Journal of security and its Applications,2016.

6] Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi.'Research on various cryptography techniques', International Journal of Recent Technology and Engineering (IJRTE), Julyb 2019.

7] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadar Hassan Disina, Zabraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris. 'A survey on the cryptography encryption algorithms', International Journal of Advanced Computer Science and Apllications(IJACSA),2017.

8] S. Karthik, and A. Muruganandam, "Data Encryption and Decryption by using Triple DES and performance analysis of crypto system," Int. J. Sci. Eng. Res., 2(11), pp. 24-31, 2014.

9] W. Stallings, and M. P. Tahiliani, Cryptography and Network Security: Principles and Practice. London: Pearson, 2014.

10] M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir, and M. Mat Deris, "A survey on the cryptographic encryption algorithms," Int. J. Adv. Computer Sci. Appl., 8(11), 2017, pp. 333-344.

11] S. Jamel, T. Herawan, and M. M. Deris, "A cryptographic algorithm based on hybrid cubes," Computational Science and Its Applications ICCSA, vol. 6019, pp. 175–187, 2010.

12] Vipin Jain.'A review on different types of cryptography techniques', ACADEMICIA: An International Multidisciplinary Research Journal SSN: 2249-7137 Vol. 11, Issue 11, November 2021.