A Review on Symmetric Key Encryption

[1]Shraddha Rajendra Kore, [2]Komal Dewadas Dhok,[3]Sonika Hanmantrao Mahind, [4]Rohit D. Mane

[1,2,3,4]Dr. J. J. Magdum College of Engineering, Jaysingpur.

Abstract

Now a day, the most important thing is to maintain confidentiality and integrity of our data. Due to the large growth of digitalization, data on internet is not secure. Cryptography is the way to secure data while transmitting from one location to another. This theory includes Encryption and Decryption. Or in other words, Encipher and Decipher. There are different types of encryption techniques, like symmetric encryption and asymmetric encryption. This paper focuses on symmetric cipher model and list out different symmetric ciphers.

Keywords

Plaintext, Ciphertext, Encryption algorithm, Secret key, Decryption algorithm.

Introduction

Cryptography is the study of information hiding and verification. When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt plain-text messages. The simplest method uses the "symmetric" or "secret key" system. *Symmetric* cryptography, also known as *secret* key cryptography, uses a single shared secret to encrypted data shared between parties. Symmetric encryption requires both the sender and receiver have the same key which is subsequently used.

A symmetric cipher is one that uses the same key for encryption and decryption. Ciphers or algorithms can be either symmetric or asymmetric. Symmetric ciphers are faster than asymmetric and allow encrypting large sets of data.

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients (As shown in Figure. A).

1. **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as an input.
2. **Encryption algorithm:** Encryption algorithm performs various substitutions and transformations on the plaintext.
3. **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations will be performed by the algorithm depend on the secret key.
4. **Ciphertext**: This is the scrambled message produced as an output of encryption algorithm. This depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, it is unintelligible.
5. **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

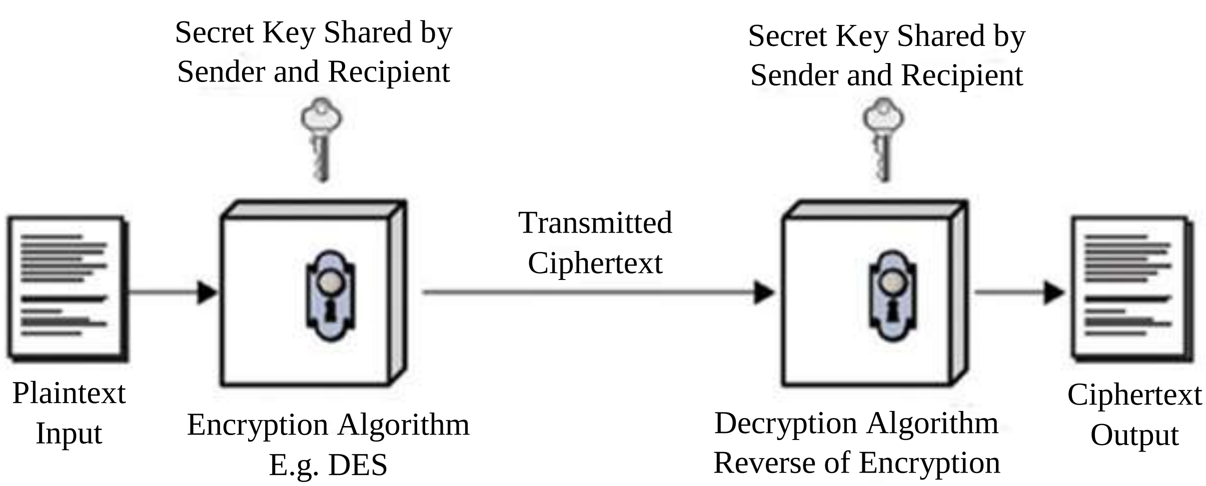
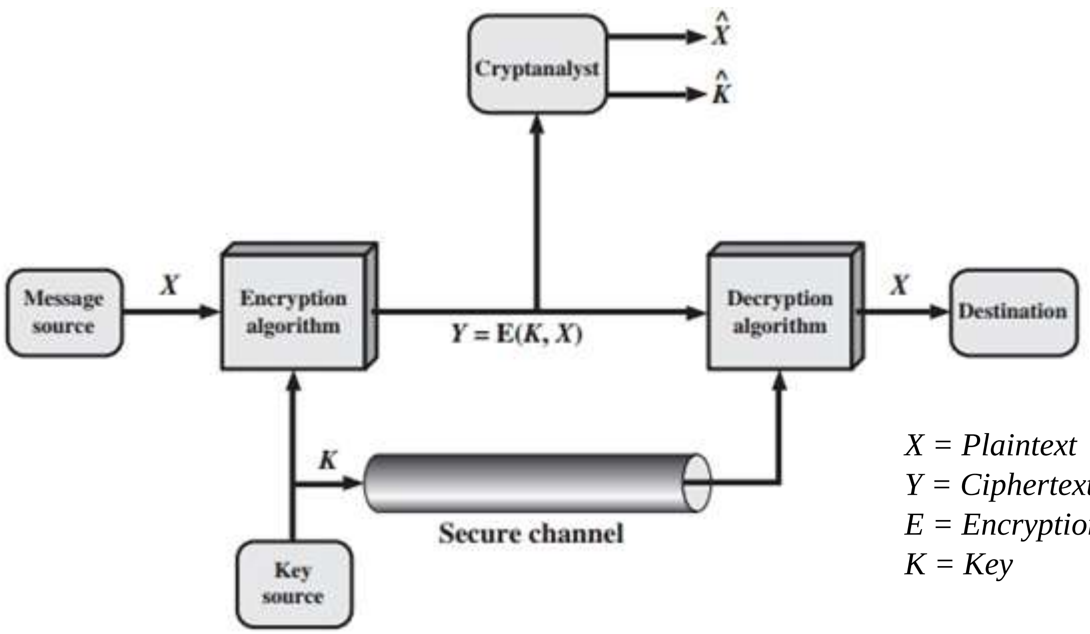


Figure-A: Symmetric Cipher Model.

There are two requirements for secure use of symmetric encryption:

1. <u>A strong encryption algorithm</u>:

We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form:



X = Plaintext
Y = Ciphertext
E = Encryption Algorithm
K = Key

Figure-B: Model of Symmetric Cipher

2. <u>Secret key known only to sender and receiver</u>:

Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

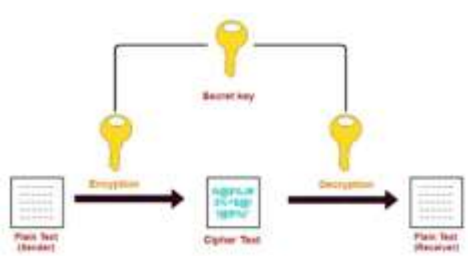


Figure C. A Cryptosystem, with the use of a Secret Key.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system [1].

Substitution technique in Symmetric Cipher: [5]

Sr. No.	Cipher Name	Invented by	Uniqueness in regards to the technique	Vulnerable to attack
1	Caesar Cipher	Julius Caesar, developed by around 100 BC	Simple alphabet substitution (Replacing each letter of the alphabet with the letter standing three places further down the alphabet)	Brute force Attack
2	Monoalphabetic Cipher	(An improvement to Caesar Cipher)	Fixed substitution, A single cipher alphabet for each plaintext alphabet is used throughout the process	Frequency Analysis
3	Playfair Cipher	British Scientist sir charles wheatstone in 1854, bears the name of his friend Boron playfair	Use two letters and Then substitute them with matrix (5x5) designed with remaining alphabets and key	Frequency Analysis , Brute force Attack
4	Hill Cipher	Mathematician lester Hill in 1929	Made from Linear algebra, Convert the plaintext to matrix based on the value of ASCII	Known plaintext Attack
5	Polyalphabetic Cipher	Leon Battista Alberti	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.	Frequency Analysis
6	One Time Pad.	Frank Miller in 1882,and reinvented in 1917. Petend :- July 22, 1919, in U.S. ,Gilbert Vernam	Just like the vigenere cipher but the size of key should be equal to the size of plaintext.	Cipher text and Key choosen

Advantages:

1) In symmetric encryption, keys are short as compared to the asymmetric encryption.
2) Symmetric encryption is fast and efficient for large amount of data.

3) It is an only system which possesses the secret key can decrypt the message.
4) It is extremely secure.

Disadvantages:

1) It cannot provide digital signature.
2) The key have to be secret at both the ends.

Conclusion

Many algorithms have been developed to satisfy the security goals that are confidentiality, integrity, non-reputation and authentication. We have to choose different encryption algorithms according to the type of data. Our purpose of this paper is to explain the basic knowledge about Symmetric Key Encryption and take overview of different symmetric ciphers.

Reference:-

1. *Cryptography-network-security-principles and practices by William Stallings-indianpdf.com_ pdf.*
2. *Bellare, Mihir, Kenneth G. Paterson, and Phillip Rogaway. "Security of symmetric encryption against mass surveillance." Advances in Cryptology CRYPTO 2014. Springer Berlin Heidelberg, 2014 1-19.*
3. *Raychev, Nikolay. "Classical cryptography in quantum context. "Proceedings of the IEEE 10 (2012): 2015.*
4. *Rebeiro, Chester, Debdeep Mukhopadhyay, and Sarani Bhattacharya. "Modern cryptography." Timing Channels in Cryptography. Springer International Publishing. 2015. 13-35.*
5. *https://www.researchgate.net/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques*_in_Cryptography