A Review Paper on Cryptographic Algorithms

Ajay N[1], Akhilesh Herkal[2], Abhishek B K[3], Venkatesh Bhat[4]
Students, Department of Computer Science and Engineering[1,2,3]
Senior Associate Professor, Department of Computer Science and Engineering[4]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *Cryptography separates the capacities for encryption, decryption and because of that many people able to encrypt the messages such a way that many people now can able to read the encrypted messages. Many security safeguards in a system or network not only fulfill their principal task but also act collectively to mutually protect one another and data security has become a main concern for everyone connected to the internet. Data security ensures that our data is only accessible by the intended receiver and prevents the alternation od the data. To achieve this level of security to our data, we can so so many algorithms and methods that are already developed so far. Cryptography to protect communications, cryptographic key, which is a piece of information, not a material object. The algorithm transforms the plaintext into the ciphertext, using a particular key.*

Keywords: Cryptography.

I. Introduction

Cryptography is derived from the word Crypt which mean Hidden and Graphy means writing. It is the method of privatising the conversation or maintaining the secrecy from any third party intervention. It was believed to be discovered during 1900 BC. The start of cryptography was back to the ancient Greek, they used a device named as cipher scytale or Cipher shift. During wars the cyptographed messages were the reliable source to share any confidential messages and many wars were won because of this. The most difficult code or most sophisticated code to crack was written by the machine called Enigma.

From back then to now the cryptography has been changed in lot many ways, as it also mean that increase in the need of the more and more security to the end users. In this new technical era it is also known as encryption. But Cryptography is the process of encrypting and decrypting. There was a time when a good quality Cryptography was only used by the governments, where the common man had no access to it. But in 1970 the developments in this field broke that rule. For the first time after that revolution those who don't belong to the government could also hold the cryptography.

This modern technology is using many cryptography everywhere. The development in networking would have been impossible if the concept of cryptography wasn't there, the concept of safe web surfing wouldn't have ever exist and the usage of the internet would have been restricted for security purpose.

There are many types of cryptography like Symmetric key, Hash Functions, and Asymmetric key cryptography. Some Symmetric key algorithms are DES, it is based on the Feistel Cipher and was used for the encryption of electronic data, it was discontinued later due to some insecurity.

Asymmetric key cryptography uses the two key method to encrypt and decrypt. And the hashing is used to reduce the data loss as much as possible during the time of security breach.

II. Literature Review

Susan et al declared that network and computer-security could be a fast-moving technology inside the Computer Science field. Computer-Security that contains a target in order that it never stops moving. The algorithmic rule and mathematic ascepts like encryptions and hashing techniques, they're the most focus of security courses. The Hackers notice ways in which to hack network systems, courses area unit created that cowl the newest quite attacks however these attacks become superannuated daily due to the responses from new security softwares, security techniques and skills tend to emerge within the apply of legal organisations, security design, network improvement.

DOI: 10.48175/IJARSCT-2862

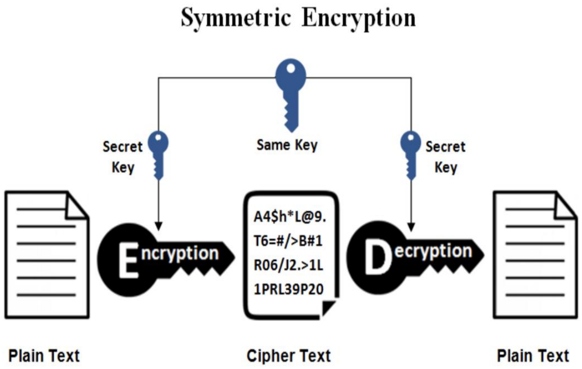
Othman O. Khalifa et al gave a concept of primary basic ideas, characteristics, and goals of cryptography. They hash out that in our age, the age of knowledge, communication has given to the expansion of technology and so has a crucial role that needs privacy to be secured and secure once knowledge is shipped through the medium of communications.

In the cryptography and network security, Sandeep Tayal et al was mentioned that with the emergence of social networks and commerce applications, immense amounts of information area unit made daily by organizations across the globe. This makes data security a large issue in terms of making certain that the transfer of information through the net is assured. With a lot of users connecting to the web, this issue additional shows the need of cryptography. This paper provides an overview of the assorted techniques utilized by networks to strengthen security, like cryptography.

Lastly, Schneier come back to associate degree finish that confidentiality of security as sensible|an honest|a decent} issue could be a story which it's not good for security to be much, as security fully counting on confidentiality is weak. If that confidentiality was lost, convalescent it might be not possible. Schneier additional expressed that cryptography supported short secret keys which will be simply transferred and adjusted should have confidence a fundamental principle, that is for the scientific discipline algorithms to be at the same time sturdy and public so as to supply smart security. the sole reliable thanks to build a lot of improvement.

II. Cryptography Concept

The basic read on cryptological system is to knowledge so as to attain privacy of the system data associate exceedingly [in a very] approach than an unauthorized person would be unable to extract its that means. 2 of the foremost common uses of cryptography would be victimization it to transfer knowledge through associate degree insecure channel, making certain that unauthorized individuals don't perceive what they're staring at in an exceedingly situation during which they need accessed the data.



In cryptography, the hid data is sometimes termed "plaintext", and also the method of disguising the plaintext is outlined as "encryption"; the encrypted plaintext is understood as "ciphertext". This method is achieved by variety of rules known as "encryption algorithms". Usually, the secret writing process depends on Associate in Nursing "encryption key", that is then provide to the encryption algorithmic program as input along side the data. Using a "decryption algorithm", the receiving facet will retrieve the information victimization the acceptable "decryption key".

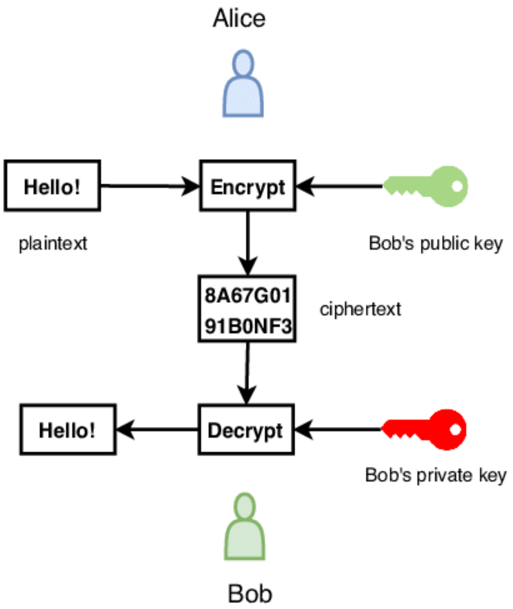
III. Cryptosystem Types

3.1 Asymmetric Cryptosystems

It use two different keys to send and receive the messages. It use public key for encryption and another key is used for decryption. Two user A and B needs to communicate, A use public key of B's to encrypt the message. B use private key to decipher the text.Itis also called as public key cryptosystems.Diffie-Hellman key exchange generate both public and private key.

3.2 Symmetric Cryptosystems

In Symmetric cryptosystems both the enciphering and deciphering keys are identical or typically each are associated with one another. Each the key ought to be unbroken safer otherwise in future secure communication won't be attainable. Keys ought to be additional secure and it ought to be changed in a secure channel between 2 users. Data Encryption customary (DES) is example of Symmetric cryptosystems.



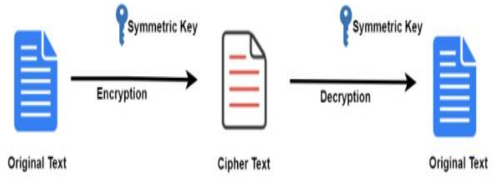


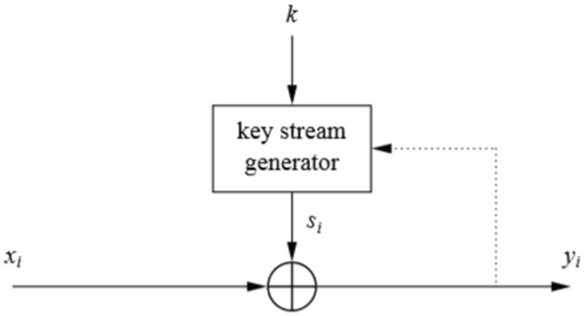
Figure: Asymmetric Cryptosystems

Figure: Symmetric Cryptosystems

IV. Modern Algorithms

4.1 Stream Ciphers

Stream ciphers treat pseudorandom bits generated from the key, and also the plaintext is encrypted by XORing each the plaintext and also the pseudorandom bits. Stream ciphers were typically avoided within the past, as they were a lot of possible than block ciphers to be broken. Nowadays, however, once years of developing styles, the stream cipher has become safer and might be trusty and relied on to be employed in connections, Bluetooth, communications, mobile 4G, TLS connections, and so on.



In a stream cipher, every bit is encrypted one by one. There area unit 2 varieties of stream ciphers: the primary is that the synchronous stream cipher, during which the key stream depends on the key; within the asynchronous cipher, though, the ciphertext relies on the key stream. In Figure three, we've got a line. If it absolutely was gift, the stream cipher would be asynchronous; otherwise it might be synchronous. The cipher feedback (CFB) would be AN example of AN asynchronous cipher

4.2 Public key systems

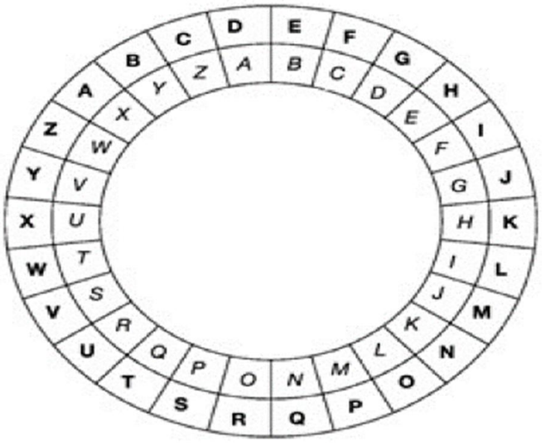
The invention of public key secret writing will be thought-about a cryptography revolution. it's obvious that even throughout the 70s and 80s, general cryptography and secret writing were alone restricted to the military and intelligence fields. it had been solely through public key systems and techniques that cryptography unfold into different areas. Public key secret writing provides US the power to ascertain communication while not betting on personal channels, because the public key will be publicized while not ever worrying concerning it. A outline of the general public key and its options follows:

1. With the utilization of public key secret writing, key distribution is allowed on public channels during which the system's initial preparation will be doubtless simplified, easing the system's maintenance once parties be a part of or leave.
2. Public key secret writing limits the necessity to store several secret keys. Even during a case during which all parties need the power to ascertain secure communication, every party will use a secure fashion to store their own personal key. the general public keys of different parties will be hold on during a non-secure fashion or will be obtained once required.
3. In the case of open environments, public key cryptography is additional appropriate, particularly once parties that haven't moved antecedent need to speak firmly and interact. for instance, a business person might have the power to reveal their public key on-line, and anyone World Health Organization needs to buy one thing will access the general public key of the businessperson as necessary once they need their master-card info encrypted.

V. Historical Algorithms

5.1 Caesar Cipher

This is one amongst the oldest and earliest samples of cryptography, fancied by solon, the emperor of Rome, throughout the Gallic Wars. during this variety of algorithmic rule, the letters A through we have a tendency to square measure encrypted by being depicted with the letters that come back 3 places previous every letter within the alphabet, whereas the remaining letters A, B, and C square measure depicted by X, Y, and Z. this implies that a "shift" of three is employed, though by mistreatment any of the numbers between one and twenty five we have a tendency to may acquire an identical result on the encrypted text. Therefore, nowadays, a shift is usually considered a Caesar Cipher.



As the Caesar cipher is one amongst the best samples of cryptography, it's easy to interrupt. so as for the ciphertext to be decrypted, the letters that were shifted get shifted 3 letters back to their previous positions. Despite this weakness, it would been robust enough in historical times once solon used it throughout his wars. Although, because the shifted letter within the Caesar Cipher is usually 3, anyone attempting to decipher the ciphertext has solely to shift the letters to decipher it.

5.2. Transposition Ciphers

Other cipher families work by ordering the letters of the plaintext to rework it to cipher text employing a key and specific rule. Transposition will be outlined because the alteration of the letters within the plaintext through rules and a particular key. A columnar transposition cipher will be thought-about mutually of the best forms of transposition cipher and has 2 forms: the primary is named "complete columnar transposition", whereas the second is "incomplete columnar". no matter that type is employed, a parallelogram form is employed to represent the written plaintext horizontally, and its dimension ought to correspond to the length of the key getting used. There will be as several rows as necessary to write down the message. once complete columnar transposition is employed, the plaintext is written, and every one empty columns area unit full of null so every column has a similar length. For Example:

```
s e c o n d
d i v i s o
n a d v a n
c i n g t o
n i g h t x
```

The cipher text is then derived from the columns depending on the key. In this example, if we used the key “321654”, the cipher text is going to be:

cvdng eiaii sdncn donox nsatt oivgh

However, once it involves AN incomplete columnar transposition cipher, the columns aren't needed to be completed, that the null characters area unit overlooked. This ends up in columns of various lengths, which may cause the ciphertext to be tougher to decipher while not the key.

REFERENCES

[1] N. Sharma , Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.

[2] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[3] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.

[4] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.

[5] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.

[6] N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .

[7] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763-770, 2017.

[8] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," International Journal of Engineering Development And Research, vol. 2, no. 2, pp. 1667-1672, 2014.

DOI: 10.48175/IJARSCT-2862