Brief History of Encryption

Dwiti Pandya
Student
Sinhgad Academy of Engineering
Pune, India

Khushboo Ram Narayan
Student
Sinhgad Academy of Engineering
Pune, India

Sneha Thakkar
Student
Sinhgad Academy of Engineering
Pune, India

Tanvi Madhekar
Student
Sinhgad Academy of Engineering
Pune, India

B.S. Thakare
Asst. Professor
Sinhgad Academy of Engineering
Pune, India

ABSTRACT

Secure communication has been required since thousands of years. This led to the invention of cryptography. In ancient world, primitive methods were adopted for passing messages secretly. But with the invention of internet and world wide web, which is used for communicating via mail, messages, online shopping, online banking, etc., increased the need of information security. Thus a proper understanding of various methods of cryptography and its implementation can fulfill the requirements of securing valuable and sensitive information. This paper takes us through the various methods of cryptography adopted in the ancient period, medieval period and the modern era.

General Terms

Cryptography, encryption, transposition ciphers, substitution ciphers, ciphertext, hieroglyphs, Atbash, scytale, monoalphabetic, enigma, encryption, rijndael, pseudorandom.

Keywords

AES, DES, MD4, RC4, SHA, SIGABA

1. INTRODUCTION

Cryptography is a way of secure transmission and storage of data such that only the party for whom it is intended can read and others cannot. Cryptanalysis is the art of breaking codes, cipher text and cryptosystems without knowing the key or algorithm. Cryptology includes the study of both cryptography and cryptanalysis. Encryption is the process of converting plaintext to cipher text with the help of suitable schemes, algorithms and key. Thus the message encrypted can only be decrypted by the intended recipient with the help of corresponding decryption algorithms and key.

The word “encryption” have come from the Greek word kryptos which means hidden. Since the earliest of times, humans have been interested in keeping certain sensitive information that they possess out of the reach of others for whom it isn’t intended. In earlier times, they used to substitute parts of the information with symbols, numbers, picture, etc. Different people have made use of cryptography for different reasons. The Assyrians wanted to protect their trade secret of manufacturing pottery. The Chinese wanted to protect their trade secret of manufacturing silk. The Germans wanted to protect their military secrets. With the advancement of computers and internet, various firms, businesses, industries, etc. had to protect their official data from intruders. In this paper, we will see how various encryption methods have been developed from earlier times to the present day.

2. ANCIENT FORM OF CRYPTOGRAPHY

The ancient form of cryptography mainly includes the classical methods. The most famous ones are the transposition ciphers and the substitution ciphers. The transposition ciphers work by rearranging the alphabets or changing the order of the alphabets appearing in a word. For example, ‘first’ becomes ‘ifrts’, whereas substitution ciphers [1] works by replacing letters or group of letters with other letters or group of letters. The first noted example of written cryptography was the ciphertext, in the form of non-standard hieroglyphs, which was carved on monuments by the Egyptians about 1900 BC. These did not provide much concealment or was not much of an attempt at secret communication, but for the amusement of literate onlookers. About 500-600 BC, Hebrew scribes came up with a simple substitution cipher known as Atbash. Atbash works by reversing the alphabets in the following manner, i.e. the letter ‘a’ is replaced by the letter ‘z’, the second letter ‘b’ is replaced by the letter ‘y’ and so on. For example, ‘world’ is replaced by ‘dliow’.

About 487 BC, the Greeks and the Spartans used the ‘scytale’ transposition cipher to secretly communicate during military campaigns. This scheme consists of a rod around which a strip of parchment or leather is wound with a message written over it. This rod is called the encryption rod. The recipient is supposed to have a rod of the same diameter and wound the parchment around it to read the message. This way others, not having the rod of same diameter, cannot read the message. The recipient’s rod is called the decryption rod.

About 100-44 BC, Julius Caesar used a simple substitution cipher to secretly communicate with his generals. So he replaced every A by a D, every B by an E, and so on. Only someone who knew the ``shift by 3" rule could decipher his message.

Table 1. Alphabet Replacement

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

3. MEDIEVAL CRYPTOGRAPHY

The classical ciphers provided concealment and enough secrecy until the frequency analysis was discovered by an Arab mathematician and polymath Al-Kindi in the 9th century (about 800 AD). Thus it had become possible to easily break the ciphers and obtain the plaintext. A book on cryptography named “Risalah fi Istikhraj al- Mu’amma” described the use of frequency analysis which was first known. In this the frequency of individual characters were observed and monoalphabetic ciphers were easily cracked.

About 1467 AD, an Italian mathematician, Leon Battista Alberti developed polyalphabetic ciphers and was given the title, “Father of Western Cryptology”. He had introduced the idea of an cipher disk. It is a device which encodes and decodes messages by use of concentric wheels inscribed with alphabets and numbers.

Between 1400s-1600s, in Europe, citizens of Italian states worked hard on cryptographic practices. The primary reasons were to communicate about various political and religious issues. About 1518, Johannes Trithemius wrote a book on cryptology, “polygraphia”[2]. He invented the tabula recta which was used in polyalphabetic ciphers like Vigenere cipher. It uses a square of 26 letters (of the alphabet) followed by 26 rows of additional letters, with each row shifted once to the left. In 1586, The Babington plot, which had an aim to assassinate Queen Elizabeth I, was unraveled by means of cryptanalysis.

3.1 Cryptography from 1800 TO World War I

It was during this period when more complex and powerful cryptography and cryptanalysis techniques were developed.

Around 1840, a well-known poet Edgar Allen Poe and a pioneer in breaking codes, had challenged the readers of Alexander’s Weekly (Express) Messenger to submit ciphered messages to him, and had been successful in solving most of them. He later wrote an essay on cryptographic methods which helped the British people to decipher German codes and cipher during World War I.

Between 1853- 1856, Charles Babbage had successfully developed techniques to break polyalphabetic ciphers like Vigenère’s autokey cipher. This had largely benefitted the British Crimean War efforts.

In 1917, Gilbert Vernam invented a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined one character at a time with the plaintext message in order to produce the ciphertext. This led to the development of electromechanical devices as cipher machines, and to the one time pad which is an unbreakable cipher[3].

3.2 World War II Cryptography

This period marked the use of more and more mechanical and electromechanical cipher machines. Major advancements in cipher design and cryptanalysis were made.

Between 1920- 1930, a cipher machine called the Enigma rotor machine was invented by Arthur Scherbius which was used by the German Army. The German military messages coded on the Enigma machine were first decoded by the Polish Cipher Bureau in 1932. Three polish cryptologists, Marian Rejewski, Jersy Rozycki and Henryk Zygalski, who worked for military intelligence, were able to do so. They were aided by the documents provided by French military intelligence and Rejewski’s reverse engineering of the machine using mathematics. Thus, they designed a mechanical device for decoding Enigma ciphers in 1938. After this, the Germans added complexity to the Enigma machines which made it difficult to break the codes with the existing resources the Polish possessed. In 1939, the Poles formed an alliance with the French and the British military intelligence. Later models, Typex machine made by the British and the SIGABA machine made by the US would improve upon the concepts of Enigma [3].

In 1942, the US Navy cryptographers broke into the Japanese Navy cryptography system, JN-25. Thus this aided them to win against the Japanese in the Battle of Midway.

During the period 1943-1944, world’s first programmable digital electronic computer “Colossus” was designed by Max Newman and Tommy Flowers, to help with Britain’s cryptanalysis.

In 1950s, the Soviets used a very complex hand cipher known as the VIC cipher, had remained unbroken during the world.

4. MODERN CRYPTOGRAPHY

By the end of the World War II the task of preparing and decrypting ciphers has shifted from machines to computers. Modern cryptography is all about using computers and mathematical functions to represent the data in a more secure way. There were many approaches to encrypt a given data. These can be categorized as:

1) Symmetric Key Algorithm

2) Public key Algorithm

4.1 Symmetric Key Algorithm

A symmetric Key algorithm uses the same parameter (key) for encryption and decryption i.e. same key is used while sending and receiving the data (if used in networking area) or the key used for encryption is different than the decrypting key but both are same as they can be computed from each other based on some mathematical function used.

The input data which is to be encrypted can be represented or used as a block (Block ciphers) or they can undergo the encryption process character-by-character (stream ciphers). Algorithms like DES and AES are block ciphers i.e. (the data is encrypted in blocks of plaintext) both uses the symmetric key concept. While algorithm like RC4 is a stream cipher. In stream cipher the obtained stream depends upon some internal function which changes as per the cipher.

Hash functions are another approach for encryption. They take the input information which might be of any length and output a message which is short and of fixed length. MD4 is a strong hash function which is now broken and MD5 a better version of MD4 is used. The US National Security Agency also have developed a Secure Hash Function series of MD5 like hash functions. Different algorithms like SHA-0, SHA-1, SHA-2, came .Each version promised an improved functionality over the other. The Hash Function design competition was organized to search for a new US standard. The search ended after finding the new SHA-3 Hash Algorithm in 2012.

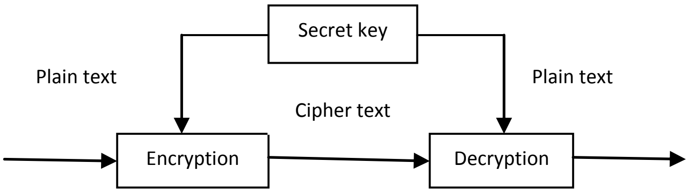

Fig 1: Symmetric key Algorithm

4.1.1 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a block cipher. DES uses a symmetric key algorithm. It is derived from Lucifer and was first published in 1975 by Federal Register US to get rid of various attacks. It is in very widespread use, like ATM encryption, also in providing mail privacy and security in remote access. DES algorithm uses the same key for encryption and decryption.

It has a key of length 56 bits and a block of 64 bits [4]. It contains 16 subkeys on for each round. Each subkey is 42 bit long. Before the processing of the 16 stages the block is divided into two halves each of 32 bits and each part is processed in alternate manner. This approach is known as Feistel scheme. In this scheme the overall process of encryption and decryption is the same only the subkeys used for the decryption process are different.

Despite all the security majors DES algorithm could not get away through several attacks as the key size used is very small .i.e. 56 bits. Many versions of DES were produced. DES -2 or Double DES is an algorithm where two different keys each of 56 bits are used .i.e. altogether the algorithm contains a key of 112 bits and 64 bits of plaintext. Even DES2 and later versions did not prove to give a fully secure algorithm. However in case of DES, Triple DES is the most secure one having extended security bur it was also later replaced by AES algorithm.

4.1.2 Advanced Encryption Standard (AES)

AES is an advanced version of DES. DES containing a fixed block size made the whole encryption process less flexible. In order to design a more flexible encryption algorithm AES was designed .AES contains different key sizes based on which different numbers of rounds are chosen. The block size used in AES is of 256 bits which eliminated the problems of the small key used in DES.

The variable size of key length makes the whole process more secure.

The variable key sizes are:

1) 64-bits having 12 rounds.

2) 128-bits having 14 rounds.

3) 256-bits having 16 rounds.

Based on the key size different number of rounds is selected which is used to encrypt a 256-bits long plaintext. The text and the key both undergo different key schedules and the data is encrypted. The decryption process uses the same number of rounds but the subkeys used are reversed.

In 1998 the National Institute of Standards and Technology (NIST/USA) announced a "competition" for a new block cipher. Fifteen algorithms were submitted to NIST from all around the world. In the summer of 2001 NIST an algorithm called Rijndael [5] was selected as the new standard. This uses AES as the base. After AES several other algorithms were produced like AES 512. This algorithm uses a block size of 512 bits and many other changes were also made.

4.2 Public key cryptography

Public key Algorithm is an approach which uses separate keys to encrypt and decrypt the data. The problem with the Symmetric key is the management of keys to use them securely. The key should be communicated first between the sender and the user in order to decrypt the information correctly. To do so a secure network is required .This is not reliable in real world. And also with problems like chicken-and-egg it is inconvenient to use symmetric key algorithm and also the risk increases with more number of users getting attached to the network. To overcome these drawbacks Whitfield Diffie and Martin Hellman proposed a public key algorithm (Asymmetric Key Algorithm) in 1976. In these algorithms two different keys which are mathematically related are used. One is a public key and the other is a private key.

In this system, even though the public keys are mathematically related with each other it is relatively infeasible to find one key (private key) from the other given public key. In public key cryptosystem, the public key is either freely distributed or can be shared secretly. But the private key should be shared with secrecy. The public key is used for encryption whereas private key is used to decrypt the information.

Diffie and Hellman put efforts to find a practical public-key encryption system. This was finally done in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution later came to know as the RSA Algorithm. This idea of using Asymmetric key gained a worldwide popularity and became the most widely used algorithm. Public key Algorithm can also be used in digital signatures.

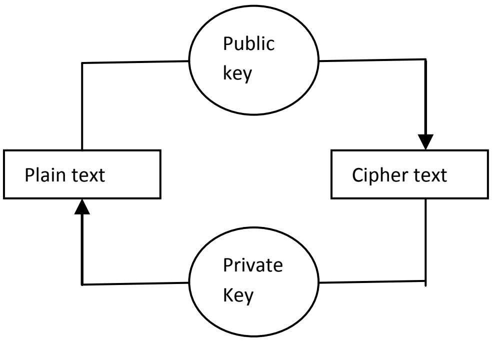

Fig 2: Public key Cryptography

5. PSEUDORANDOM

The disadvantage of Modern Cryptographic approach is that the key (our one time pad) used is almost the same size as the message. So In order to increase the security we need a system which can generate a random string. But such a generator is not possible. Any such generator will produce a normal string which may not be random. So the concept of strings arises that appears to be random. The bits are said to be *pseudorandom* [6]. The general idea behind this is that the bits are not really random but they are as good as random so we can use them for our purpose. In this case mostly the same string is repeated and different collection of bits is chosen at a time and that is the reason it appears to be randomly generated. This provides a significant amount of security to the system.

6. CONCLUSION

Cryptography and its techniques have been evolving since a long time now. It started with primitive methods in which the algorithms/methods were required to be kept secret. If the algorithm was known, then it was simple to decrypt the message. But with time, new methods evolved whose algorithms were kept open in public and yet decrypting the message proved difficult and required skills. Today AES has proved to be the most advanced and secure encryption method. The research in this field is still in process and the efforts to find even more secure and optimized is still in the run.

7. REFERENCES

[1] "History of cryptography." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 5th November 2015. Web. 10th November 2015. < https://en.wikipedia.org/wiki/History_of_cryptography>

[2] "Cryptography." Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 27th November 2015. Web. 29thNovember2015.<https://en.wikipedia.org/wiki/Cryptography>

[3] *The Evolution of Cryptography*. (n.d.). Retrieved November12,2015,fromhttp://www.sherpasoftware.com/blog/the-evolution-of-cryptography/

[4] Bellare, M., Rogaway, P., 2005. Introduction to modern cryptography.

[5] J. Daemen and V. Rijmen. The Design of Rijndael. Springer, 2001.

[6] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput*, Vol. 17, No. 2, April 1988.