International Journal For Technological Research In Engineering
Volume 4, Issue 8, April-2017 *ISSN (Online): 2347 - 4718*

HISTORY OF CRYPTOGRAPHY

Prof.Waghmare S.P[1], Simran Sikhwal[2], Shreyas Nimje[3], Tanvi Pawar[4]
Bharati Vidyapeeth College Of Engg, Kharghar, Navi Mumbai (India)

Abstract: ***Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.***

Keywords: Cryptography, Decryption, Encryption, Cipher text, Classic Cryptography, E-Commerce

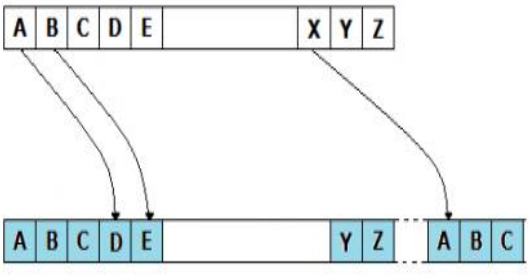
I. INTRODUCTION

The main context of the encryption/decryption program implementation is the creation of encryption key. Now a day, cryptography has many commercial uses. If we are protecting secret information then cryptography is needed at high level of privacy of individuals and groups. However, the main purpose of cryptography is used not only to provide secretly, but also to give solution for other problems like: data integrity, authentication, non-repudiation1. Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

II. HISTORY OF CRYPTOGRAPHY

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext).[2] Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Formally, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication.[3] Examples of asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).[4]

The first known evidence of the use of cryptography (in some form) was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. The scribe used some unusual hieroglyphic symbols here and there in place of more ordinary ones. The purpose was not to hide the message but perhaps to change its form in a way which would make it appear dignified. Though the inscription was not a form of secret writing, but incorporated some sort of transformation of the original text, and is the oldest known text to do so. Evidence of some use of cryptography has been seen in most major early civilizations. "Arthshashtra", a classic work on statecraft written by Kautalya, describes the espionage service in India and mentions giving assignments to spies in "secret writing" - sounds like an ancient version of James Bond.[5]



Classic Cryptography

The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military).[6] Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, was a message tattooed on a slave's shaved head and concealed under the regrown hair.[2] More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information. Ciphertexts produced by a classical cipher (and some modern ciphers) will reveal statistical information about the plaintext, and that information can often be used to break the cipher. After the discovery of frequency analysis, perhaps by the Arab mathematician and polymath Al-Kindi (also known as Alkindus) in the 9th century,[7] nearly all such ciphers could be broken by an informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles (see cryptogram). Al-Kindi wrote a book on cryptography entitled Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages), which described the first known use of frequency analysis cryptanalysis techniques.[7][8]

First page of a book by Al-Kindi which discusses encryption of messages

III. COMPUTER ERA

Cryptanalysis of the new mechanical devices proved to be both difficult and laborious. In the United Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient means for carrying out repetitious tasks. This culminated in the development of the Colossus, the world's first fully electronic, digital, programmable computer, which assisted in the decryption of ciphers generated by the German Army's Lorenz SZ40/42 machine. Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s. In recent times, IBM personnel designed the algorithm that became the Federal (i.e., US) Data Encryption Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm;[9] and the RSA algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography has become a widely used tool in communications, computer networks, and computer security generally. Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. There are very few cryptosystems that are proven to be unconditionally secure. The one-time pad is one. There are a few important ones that are proven secure under certain unproven assumptions. For example, the infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and some other systems, but even there, the proof is usually lost due to practical considerations. There are systems similar to RSA, such as one by Michael O. Rabin that is provably secure provided factoring n = pq is impossible, but the more practical system RSA has never been proved secure in this sense. The discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again, there are related, less practical systems that are probably secure relative to the discrete log problem.[10]

IV. RESULT

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

V. CONCLUSION

After going through the history of cryptography eventually it had proved its enormous role in the modern age with the help of computer coding, digital algorithm & it is the one of the most advance tool in the security of internet like for the protection of financial transaction for banking shopping then information storage of all retrievals processing & government application. It will also more technically convenient & advance with the safe implementation of complex mathematical equation & protocols. Authors are working on its future aspects.

REFERENCE

[1] Prof. S.P. Waghmare ,Study of Mathematical cryptography part modern era.ISBN 978-93-8601-12-2, ICRTESM 16

[2] Kahn, David (1967). The Codebreakers. ISBN 0-684-83130-9

[3] An Introduction to Modern Cryptosystems".

[4] Sharbaf, M.S. (2011-11-01). "Quantum cryptography: An emerging technology in network security". 2011 IEEE International Conference on Technologies for Homeland Security Red Hat ¸Published on august 14, 2013

[5] Ashchenko, V. V. (2002). Cryptography: an introduction

[6] Singh, Simon (2000). The Code Book. New York: Anchor Books

[7] Al-Kadi, Ibrahim A. (April 1992). "The origins of cryptology: The Arab contributions". Cryptologia

[8] Diffie, Whitfield; Hellman, Martin (November 1976). "New Directions in Cryptography" (PDF). IEEE Transactions on Information Theory. IT-22: 644–654

