Opinion
Volume 15:1, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

Cryptography and its Application

Sanika Swapna*

Department of Biotechnology, Osmania University, Hyderabad, Telangana, India

Opinion

The study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents is known as cryptography. The word comes from the Greek word kryptos, which means "hidden." It is closely related to encryption, which is the act of scrambling plain text into cipher text and then back again when it arrives. Furthermore, cryptography includes the obfuscation of information in images through the use of techniques such as microdots or merging. The ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with inventing one of the first modern cyphers.

Encrypting and decrypting email and other plain-text messages is the most common use of cryptography when transmitting electronic data. The symmetric or "secret key" system is the most basic method. Data is encrypted using a secret key in this case, and both the encoded message and the secret key are then sent to the recipient for decryption. What's the issue? If the message is intercepted, a third party has all the information they need to decrypt and read it. Cryptologists devised the asymmetric or "public key" system to address this issue. Every user in this case has two keys: one public and one private. Senders request the recipient's public key, encrypt the message, and send it on.

Symmetric Key Cryptography is an encryption system in which the sender and receiver use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler, but the sender and receiver must exchange keys in a secure manner. Data Encryption System is the most widely used symmetric key cryptography system (DES). Hash Functions No keys are used in this algorithm. A hash value with a fixed length is calculated based on the plain text, making it impossible to recover the plain text's contents. Many operating systems encrypt passwords using hash functions.

Asymmetric Key Cryptography, This system encrypts and decrypts data using a pair of keys. For encryption, a public key is used, and for decryption, a private key is used. There is a distinction between a public key and a private key. Even if everyone knows the public key, the intended receiver can only decode it because he is the only one who knows the private key. A transposition cypher is a method of encryption in which the positions of plaintext units (typically characters or groups of characters) are shifted according to a regular system, resulting in cipher text that is a permutation of the plaintext.

That is, the order of the units has been altered. To encrypt, an objective function on the positions of the characters is used, and to decrypt, an inverse function is used. An encryption method that encrypts a block of text using a deterministic algorithm and a symmetric key, rather than encrypting one bit at a time as in stream cyphers. Encrypts a single bit at a time using a symmetric or secret-key encryption algorithm. A Stream Cipher encrypts the same plaintext bit or byte to a different bit or byte each time it is encrypted.

References:

1. Hasan M, Anwarul, Muzhong Wang, and Vijay K Bhargava. "Modular construction of low complexity parallel multipliers for a class of finite fields GF(2^m)." *IEEE Trans Comput* 41 (1992): 962-971.
2. Itoh, Toshiya. "Characterization for a family of infinitely many irreducible equally spaced polynomials." *Inf Process Lett* 37 (1991): 273-277.
3. Itoh, Toshiya and Shigeo Tsujii. "A fast algorithm for computing multiplicative inverses in GF (2m) using normal bases." Inf Comput 78 (1988): 171-177.
4. Wu, Huapeng and M Anwarul Hasan. "Low complexity bit-parallel multipliers for a class of finite fields." *IEEE Trans Comput* 47 (1998): 883-887.
5. Paar, Christof. "A new architecture for a parallel finite field multiplier with low complexity based on composite fields." *IEEE Trans Comput* 45 (1996): 856-861.

How to cite this article: Swapna, Sanika. "Cryptography and its Application." J Comput Sci Syst Biol 15 (2022):396.

Address for Correspondence: *Sanika Swapna, Department of Biotechnology, Osmania University, Hyderabad, Telangana, India, E-mail: sanika.swapna25@gmail.com*

Received 03-Jan-2022, Manuscript No. jms-22-56309; **Editor assigned:** 05-Jan-2022, Pre QC No. P-56309; **Reviewed:** 17-Jan-2022, QC No.Q-56309; **Revised:** 22-Jan-2022, Manuscript No.R-56309 **Published:** 29-Jan-2022, DOI: 10.37421/jms.2022.11. 396.