Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-11, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

A Survey on Methods of Cryptography and Data Encryption

Prof. Swapnil Chaudhari [1], Mangesh Pahade [2] , Sahil Bhat [3]
Tejaswini Sawant [4]& Chetan Jadhav [5]
[1]Assistant Professor Computer Engg. Dept., SPPU University, Pune, India
[2,3,4,5] B.E Computer Engg. (Final Year), SPPU University, Pune, India

Abstract: *In today's world Sensitive data are increasingly used in communication over internet. Thus Security of data is biggest concern of internet users. Best solution is use of some cryptography algorithm which encrypts data in some cipher and transfers it over internet and again decrypted to original data. The field of cryptography deals with the procedure for conveying information securely. The goal is to allow the intended recipients of a message to receive the message properly while interrupt eaves-droppers from understanding the message. Key arrangement schema allows communicating parties to establish a shared cipher key. This paper provides survey to data security problem through Cryptography technique. Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data classified and for verifying data indignity.*

Keywords- *PS; Encryption; ASCII; Genetic algorithm CIPHER.*

1. Introduction

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the “security threat” it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most necessary factors that need attention during the process of data transferring. Cryptography is the science or study of techniques of secret writing and message hiding. Cryptography is as broad as formal lexemic which obscures the method in which someone attempts to hide a message, or the meaning there of, in some medium.

. Encryption is one specific element of cryptography in which one hides data or information by transforming it into an unreadable code. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. Decryption is often restricted along with encryption as it's opposite. Decryption of encrypted data results in the original data.

. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general preservation of company data and interchange secrets. If this data needs to be viewable, it may require decryption. If a decryption pass code or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

. A cipher is an algorithm, process, or method for performing encryption and decryption. A cipher has a set of well-defined steps that can be followed to encrypt and decrypt messages. The operation of a cipher usually depends largely on the use of an encryption key. The key may be any spare information added to the cipher to produce certain outputs.

. Un-encrypted text or message in its original-human readable-form Plain text is the input of an encryption process, and the output of a decryption process. Also called clear text, it is the opposite of cipher text.

2. Symmetric and Asymmetric method.

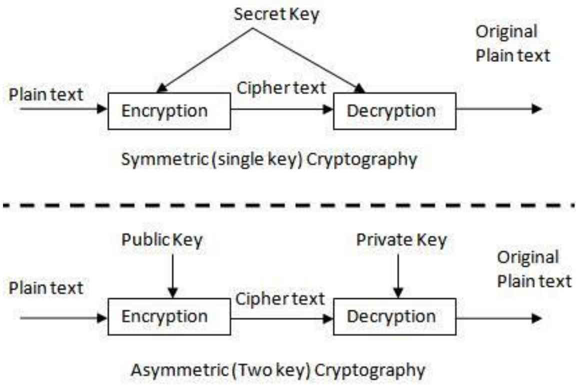

Fig:-Symmetric and Asymmetric System Model

- **Cipher** An algorithm for performing encryption (and the reverse, decryption) - a series of well-defined steps that can be followed as a procedure. Works at the level of individual letters, or small groups of letters.

- **Cipher text** A text in the encrypted form produced by some cryptosystem. The convention is for cipher texts to contain no white space or reference.

- **Cryptography** The process or skill of communicating in or deciphering classified scripts or ciphers.

- **Cryptosystem** The package of all processes, formulae, and instructions for encoding and decoding messages using cryptography.

- **Decryption** Any procedure used in cryptography to convert cipher text (encrypted data) into plaintext.

- **Encryption** The process of putting text into encoded form.

- **Cryptanalysis** The analysis and deciphering of cryptographic writings or systems.

- **Plaintext** A message before encryption or after decryption, i.e., in its usual form which anyone can read, as opposed to its encrypted form.

4. Symmetric Algorithm

4.1. AES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data. The Advanced Encryption Standard was originally known as Rijndael. Rijndael algorithm is symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits, which is specified by the flips standard. Rijndael was designed to handle additional block sizes and key lengths however; they are not adopted by this standard. Throughout the remainder of this presumption, the algorithm specified herein will be referred to as “the AES algorithm”. The algorithm may be used with the three different key lengths indicated above, and therefore these different “flavors” may be referred to as “AES-128”, “AES-192” and “AES-256”.

4.2. DES

The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

4.3. Blow Fish

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. (The U. S. government forbids the exploitation of encryption software using keys larger than 40 bits except in special cases.) Blowfish was designed in 1993 by Bruce Schneider as an alternative faster than DES. Since its origin, it has been analyzed considerably. Blowfish is untainted, license-free, and available free for all uses.

4.4. Triple-DES

Triple-DES is a way to make the DES dramatically more secure by using the DES encryption algorithm three times with three different keys, for a total key length of 168 bits. Also called "3DES," this algorithm has been widely used by financial institutions and by the Secure Shell program (ssh). Simply using the DES twice with two different keys does not improve its security to the extent that one might at first suspect because of a logical plaintext attack called *meet-in-the-middle*, in which an assaulter simultaneously attempts encrypting the plaintext with a single DES operation and decrypting the cipher text with another single DES operation until a match is made in the middle.

4.5. Advantages of Symmetric Algorithm

- A symmetric cryptosystem is faster.
- A symmetric cryptosystem uses countersign.
- Authentication to prove the receiver's identity.

4.6. Disadvantages of Symmetric Algorithm

- Symmetric cryptosystems have a problem of key transportation.
- Secure way of exchanging keys would be commute them personally.
- Cannot provide digital signatures that cannot be repudiated.
- The secret key is to be transmitted to the receiving system before the actual message is to be conveyed.
- Symmetric ciphers require a secret channel to send the secret key-generated at one side of the channel to the other side.

5. Asymmetric Algorithm

5.1. RSA

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Aleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Many protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. It is also used in software programs-browsers are an noticeable example, which need to build a secure connection over an insecure network like the Internet or validate a digital signature. RSA signature verification is one of the most commonly performed operations in IT.

5.2. DSA

A Digital Signature Algorithm (DSA) refers to a standard for digital signatures. It was introduced in 1991 by the National Institute of Standards and Technology (NIST) as a better method of creating digital signatures. Along with RSA, DSA is considered one of the most preferred digital signature algorithms used today. DSA, on the other hand, does not encrypt message digests using private key or decrypt message digests using public key. Instead, it uses unique mathematical functions to create a digital signature consisting of two 160-bit numbers, which are originated from the message brief and the private key. DSAs make use of the public key for authenticating the signature, but the authentication process is more difficult when compared with RSA.

5.3. Diffie-Hellman key

Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would be code break mathematically overwhelming.

To implement Diffie-Hellman, the two end users Alice and Bob, while communicating over a channel they know to be private, mutually agree on positive whole numbers p and q, such that p is a prime number and q is a generator of p. The generator q is a number that, when raised to positive whole-number powers less than p, never produces the same result for any two such whole numbers. The value of p may be large but the value of q is usually small.

Once Alice and Bob have agreed on p and q in private, they choose positive whole-number personal keys a and b, both less than the prime-number modulus p. Neither user reveal their personal key to anyone; ideally they cram these numbers and do not write them down or store them anywhere. Next, Alice and Bob compute public keys $a^*$and b^* based on their personal keys according to the formulas:

$$a^* = q^a \bmod p$$

and

$$b^* = q^b \bmod p$$

The two users can share their public keys a^* and b^* over a communications medium pretended to be insecure, such as the Internet or a corporate wide area network (WAN). From these public keys, a number x can be generated by either user on the basis of their own personal keys. Alice computes x using the formula:

$$x = (b^*)^a \bmod p$$

Bob computes x using the formula

$$x = (a^*)^b \bmod p$$

The value of x turns out to be the same according to either of the above two formulas. However, the personal keys a and b, which are critical in the calculation of x, have not been transmitted over a public medium. Because it is a large and apparently random number, a potential hacker has almost no chance of correctly assuming x, even with the help of a powerful computer to conduct millions of trials. The two users can therefore, in theory, communicate privately over a public medium with an encryption method of their choice using the decryption key x.

5.4. Advantages of Asymmetric Algorithm

- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eradicate the key distribution problem.
- The private keys do not ever need to be conveyed or revealed to anyone.
- Can provide digital signatures that can be discredited.
- Asymmetric ciphers also create minor key-management problems than symmetric ciphers.
- No secret channel is necessary for the exchange of the public key.

5.6. Disadvantages of Asymmetric Algorithm

- Using public-key cryptography for encryption is speed.
- Secure way of exchanging keys would be exchanging them individually.

6. Future Scope

In today’s world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information. As a result cryptography is emerging as the foundation for enterprise data security and compliance, and quickly becoming the foundation of security best practice. Cryptography, once seen as a specialized, cryptic discipline of information security, is finally coming of age.

At the end of the day we need to protect our data. Increasingly, encryption is being seen as the best way to ensure that data is protected, but the ever growing use of encryption creates a management challenge. The challenge, however, doesn’t need to be daunting. Implementing a flexible and extensible solution that automates many of the time-consuming and error-prone key management tasks in an automated enterprise-wide manner is rapidly becoming a priority for many organizations.

7. Conclusion

Cryptography algorithm is the science in secret code. Cryptography is a engine which may ease many of the anticipated problems of using the Internet for communication. However, cryptography requires the safe implementation of complex mathematical equations and protocols, and there are always worries about bad implementations. A further worry is that users are integral to securing communications, since they must provide applicable keys. A safe application of cryptographic technology will pay close attention to how public keys are associated with user identities, how stolen keys are detected and revoked and how long a stolen key is useful to a criminal. Cryptography may be splendid technology, but since security is a human issue, cryptography is only as good as the practices of the people who use it The complexity of cryptography effectively puts it outside the understanding of most people and so motivation for the practices of cryptographic security is not available. Thus our survey has both types of cryptography (symmetric& asymmetric) have their advantages and disadvantages, and out of these two algorithm will generate desired result for our recommended system.

8. References

[1] RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p Megha Nema, Shalini Stalin (Embedded tutorial: Applications of reversible logic in cryptography and coding theory, Rovin Tiwari Department of Electronics communication Engineering, SISTec, Bhopal (M.P.), India 2015).

[2] Madhumita, and Atul Nag. ”Plain Text Encryption Using AES, DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux.”Advances in Computing and Communication Engineering (ICACCE), 2015 Second International Conference on. IEEE, (2015).

[3] Ravi shankar Dhakar P Sharma Amit K Gupta "Modified RSA encryption algorithm" Second international conference on advanced computing technology(2012).

[4] Abdulameer K. Hussain "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbour Algorithm" IJCSI.