International Journal of Advanced Engineering Research and Science (IJAERS) *Special Issue (NCCSIGMA-16)*
https://dx.doi.org/10.22161/ijaers/si.14 *ISSN: 2349-6495(P) | 2456-1908(O)*

Cipher Text Design with Asymmetric RSA Algorithm

S.Divya[1], B.Deepthi Reddy[2], D.Sravanthi[3]

[1] Department of CSE, VJIT, HYD,India
Email: divya88.smile@gmail.com
[2]Department of CSE, VJIT, HYD,India
Email: deepthi.bhonagiri@gmail.com
[3]Department of IT, JBIET, HYD,India
Email:sravzsai@gmail.com

Abstract*—In today's computer-centric world, the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free cryptography is most often associated with scrambling plaintext into cipher text. Individuals who practice this field are known as cryptographers. 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. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business. This paper is to provide digital signatures that can be repudiated and increase security.*

Keywords---Cipher, Cryptography, Plain text, Cipher text, Encryption, Decryption, Symmetric, Asymmetric and RSA.

I. INTRODUCTION

In cryptography, cipher text or cypher text is the result of encryption performed on plaintext using an algorithm, called a cipher. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning cipher text into readable plaintext. Cipher text is not to be confused with code text because the latter is a result of a code, not a cipher.

1.1 Cipher

A cipher[1] (pronounced SAI-fuhr) is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself although here the term cipher text is preferred. Its origin is the Arabic *sifr*, meaning *empty* or *zero*. In addition to the cryptographic meaning, cipher also means (1) someone insignificant, and (2) a combination of symbolic letters as in together weaving of letters for a monogram.

1.2 Codes and Ciphers

Codes and Ciphers[8] are forms of cryptography, a term from the Greek *kryptos*, hidden, and *graphia*, writing. Both transform legible messages into series of symbols that are intelligible only to specific recipients. Codes do so by substituting arbitrary symbols for meanings listed in a codebook; ciphers do so by performing rule-directed operations directly on original message text. Because codes can only communicate concepts that are listed in their codebooks, they have limited flexibility. Rather, modern cryptography relies almost entirely on ciphers implemented by digital computers, and is widely employed in industry, diplomacy, espionage, warfare, and personal communications.

1.3 Plain Text

Plaintext is information a sender wishes to transmit to a receiver. *Clear text* is often used as a synonym. Plaintext has reference to the operation of cryptographic algorithms, usually encryption algorithms, and is the input upon which they operate. With the advent of computing the definition of plaintext expanded to include any data, including binary files, in addition to simple messages and human-readable documents, in a form that can be interpreted or used without needing to be processed using information not generally available (a key). The information, which would normally be called a message, document, file, etc., if to be communicated or stored in encrypted form is referred to as plaintext.

1.4 Cipher Text

Cipher text is encrypted text. Plaintext is what you have before encryption, and cipher text is the encrypted result. The term cipher is sometimes used as a synonym for

https://dx.doi.org/10.22161/ijaers/si.14 *ISSN: 2349-6495(P) | 2456-1908(O)*

cipher text, but it more properly means the method of encryption rather than the result.

Some ciphers work by simply realigning the alphabet (for example, A is represented by F, B is represented by G, and so forth) or otherwise manipulating the text in some consistent pattern. However, almost all serious ciphers use both a key(a variable that is combined in some way with the unencrypted text) and an algorithm (a formula for combining the key with the text). A block cipher is one that breaks a message up into chunks and combines a key with each chunk (for example, 64-bits of text). A stream cipher is one that applies a key to each bit, one at a time. Most modern ciphers are block ciphers.

1.5 Encryption

In cryptography[2], encryption is the process of encoding messages or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it.

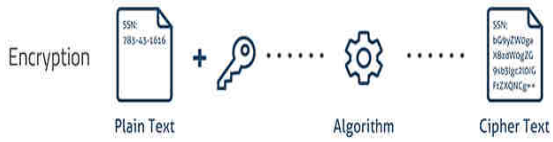

Fig. 1: Encryption Process

The purpose of encryption is to ensure that only somebody who is authorized to access data (e.g. a text message or a file), will be able to read it, using the decryption key.

1.6 Decryption

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.

Fig. 2: Decryption Process

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade 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.

II. RELATED WORK

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, Cannot provide digital signatures that cannot be repudiated and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses, Can provide digital signatures that can be repudiated and increase security.

2.1 Symmetric Key Cryptography

Symmetric algorithms[2] use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key).

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

Some examples of popular symmetric algorithms (symmetric-key algorithms):

AES/Rijndael, DES, IDEA, RC2, RC4, RC6, Triple DES, Two fish etc.

A symmetric cryptosystem is faster and encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.

Main advantages of symmetric algorithms are its security and high speed, Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only

https://dx.doi.org/10.22161/ijaers/si.14 *ISSN: 2349-6495(P) | 2456-1908(O)*

secure way of exchanging keys would be exchanging them personally, Cannot provide digital signatures that cannot be repudiated.

2.2 DES(Data Encryption Standard):

DES is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data. The only problem with this technique is that if the key is known to others the entire conversation is compromised. In this, the block size is 64 bits it also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key basically consists of 64 bits however, only 56-bits of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56-bits, and it is always quoted as such. Every 8th bit of the selected key is discarded i.e., positions 8,16, 24, 32, 40, 48, 56, 64 are removed from the 64-bit key leaving behind only the 56-bit key.

Advantages:

1. DES has been around a long time (since 1977), even now no real weaknesses have been found: the most efficient attack is still brute force[6].
2. DES is an official United States Government standard; the Government is required to re-certify, DES every five years and ask it be replaced if necessary. DES has been re-certified in 1983, 1987, 1992.
3. DES is also an ANSI and ISO standard - anybody can learn the details and implement it.
4. Since DES was designed to run on 1977 hardware, it is fast in hardware and relatively fast in software.

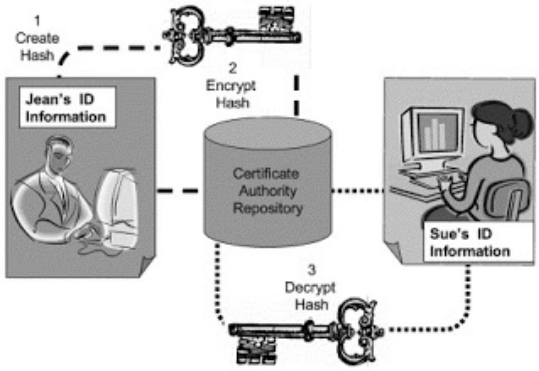

Fig. 3: DES Encryption and Decryption Process

Disadvantages:

1. The 56-bit key size is the biggest defect of DES.
2. Hardware implementations of DES are very fast[6]; DES was not designed for software and hence runs relatively slowly.
3. As we know in DES only one private key is used for encryption as well as for decryption because it is symmetric encryption technique so if we lost that key to decrypt the data then we cannot get the readable data at the receiving end.

III. PROBLEM DEFINITION

3.1 Asymmetric Key Cryptography

Asymmetric algorithms[6] use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

Asymmetric algorithms encrypt and decrypt with different keys. Data is encrypted with a public key, and decrypted with a private key. Asymmetric algorithms (also known as public-key algorithms) need at least a 3,000-bit key to achieve the same level of security of a 128-bit symmetric algorithm. Asymmetric algorithms are important because they can be used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private.

3.2 RSA Algorithm: It is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Step1: Select two large prime numbers p,q
Step2: Compute n = p*q and v = (p-1) (q-1)
Step3: Select small odd integer k relatively prime to v, gcd (k,v) = 1
Step4: Compute d such that (d*k) % v = (k*d) %v = 1
Step5: whereas public key is (k,n) and public key is (d,n)

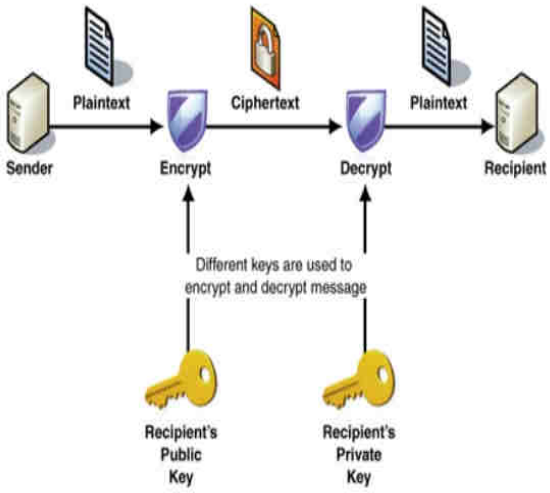

Fig. 4: RSA Encryption and Decryption Process

https://dx.doi.org/10.22161/ijaers/si.14 *ISSN: 2349-6495(P) | 2456-1908(O)*

RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

IV. CONCLUSION

This paper is for assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem. The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone. It can provide digital signatures that can be repudiated.

REFERENCES

[1] Jeffery Yi, "Cryptanalysis of Homophonic Substitution-Transposition Cipher" (2014), master's projects.
[2] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975-8887), vol-1 N0. 15.
[3] Carsten Maartmann-Moea,Steffen E. Thorkildsenb, Andre´ A˚ rnesc, "The persistence of memory: Forensic identification and extraction of cryptographic keys" from the proceedings of The Digital Forensic Research Conference DFRWS 2009 USA, Montreal, Canada (Aug 17th - 19th).
[4] Priya jaiswal, Randeep kaur, Ashok Verma, "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)
[5] Govind Prasad Arya, Aayushi Nautiyal, Ashish Pant, Shiv Singh & Tishi Handa, "A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations" The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.
[6] MargaretRouse,"Cipher", http://searchsecurity.techtarget.com/definition/cipher Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems
[7] Dorn Vernessa Samuel, "Forensic Science and Communications,Research and Technology, Code Breaking in Law Enforcement" April 2006 - Volume 8 - Number
[8] Larry Gilman, "Codes and Ciphers"
[9] Kartik Krishnan, Computer Networks and Computer Security Mar 8-11 2004