Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Apeksha Khanorkar, IJPRET, 2014; Volume 2 (9): 1089-1097 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON A NETWORK SECURITY WITH CRYPTOGRAPHY

APEKSHA A. KHANORKAR, PROF. DR. H. R. DESHMUKH, MR. R. G. ANANT WAR, MS. R. N. GADBAIL

Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Cryptography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields. They are used to protect e-mail messages, credit card information, corporate data, etc. In this paper we describe a method for integrating together cryptography and through messages. In particular, we present a system that able to perform and cryptography at the same time using messages as cover objects for and as keys for cryptography. It is shown that such system is an effective one by making a comparison with the well known RSA algorithm and is also a theoretically unbreakable cryptographic one by demonstrating its equivalence to the casier cipher.

Keywords: Facial Recognition, Face Detection, Security, Authentication, Database

PAPER-QR CODE

Corresponding Author: MS. APEKSHA A. KHANORKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Apeksha Khanorkar, IJPRET, 2014; Volume 2 (9): 1089-1097

INTRODUCTION

Security is a broad topic and covers a multitude of sins .Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone .The requirement of information security has undergone two major changes in last two decades. In earlier days cabinets with a combination lock for storing sensitive documents were used. With Introduction of computer, the need for automated tools for protecting files and other information became evident. This is very important in case of shared systems as well as for data network or internet. The generic term for the collection of the tools designed to protect data and thwart hackers is Computer Security.System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. In Network Security Cryptography play Important role as an encryption and decryption. Network Security Provide to user two keys such as private key and public key. Cryptography provides most of the methods and techniques for a secure communication. Data is Encrypted by using public keys and Data is Decrypted by using private keys. Cryptography and steganography are widely used techniques that manipulate information in orde to cipher or hide their existence. They are used to protect e-mail messages,credit card information, corporate data, etc. cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity,entity authentication, and data origin authentication. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. The former denotes the set of methods for obtaining the meaning of encrypted information. .Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by any-one except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers .Cryptology embraces both cryptography and cryptanalysis. A related discipline is steganography which is the science of hiding messages rather than making them unreadable. Steganography is not cryptography; it is a form of coding. It relies on the secrecy of the mechanism used to hide the message. If, for example, you encode a secret message by putting each letter as the first letter of the first word of every sentence, it's secret until someone knows to look for it, and then it provides no security at all.

LITERATURE REVIEW:

❖ **NEED OF CRYPTOGRAPHY:**

Confidentiality is a service used to keep the content of information from all but those authorized to posses it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible. Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution. Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed). Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving is needed to resolve the dispute. Steganography is the art and science of communicating in a way which hides the existence of the communication. The aim of this paper is to describe a method for integrating together cryptography and steganography through image processing. In particular, we present a system able to perform steganography and cryptography at the same time.

❖ **TYPES OF CRYPTOGRAPHY:**

1.SECRET KEY CRYPTOGRAPHY:

In cryptographic the term *key* refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Secret key cryptography is known *as* symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

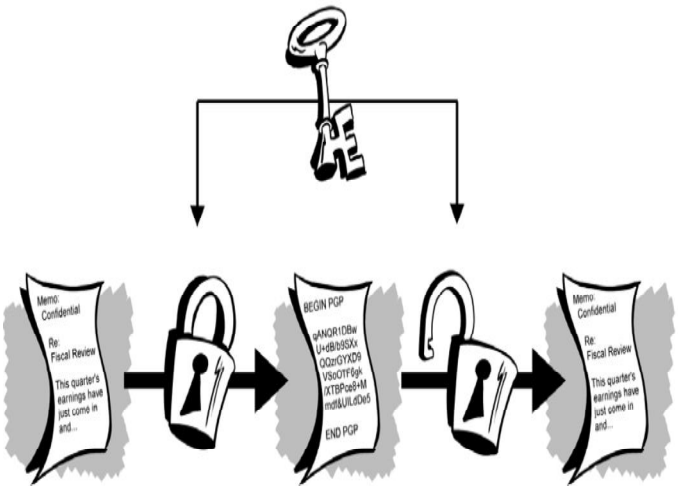

Fig 1. SYMMETRIC CRYPTOGRAPHY

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely. It is a knwon type of a crypto.

2. PUBLIC KEY CRYPTOGRAPHY:

Public key cryptography, also called asymmetric encryption, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key. The following example illustrates how public key cryptography works Ann wants to communicate secretly with Bill. Ann encrypts her message using Bill's public key (which Bill made available to everyone) and Ann sends the scrambled message to Bill.

- When Bill receives the message, he uses his private key to unscramble the message so that he can read it.
- When Bill sends a reply to Ann, he scrambles the message using Ann's public key.
- When Ann receives Bill's reply, she uses her private key to unscramble his message.

The major advantage asymmetric encryption offers over symmetric key cryptography is that senders and receivers do not have to communicate keys up possible using the public keys. PKC i.e public key cryptography turned out to be very beneficial for issues such as key distribution,

authentication etc. In the recent years first research groups started to cope with the challenges applying PKC in resource-constrained environments. One result is that in particular ECC. Public-key cryptography, refers to a cryptographic algo which requires two separate keys, one of which is *secret* (or *private*) and one of which is *public*. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature whereas the private key is used to decrypt ciphertext or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys– a public encryption key and a private decryption key. Similarly, a key pair used for digital signatures consists of a private signing key and a public verification key. The public key is widely distributed, while the private key is known only to its proprietor. The keys are related mathematically, but the parameters are chosen so that calculating the private key from the public key is either impossible or prohibitively expensive. *Public-key encryption*, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key.

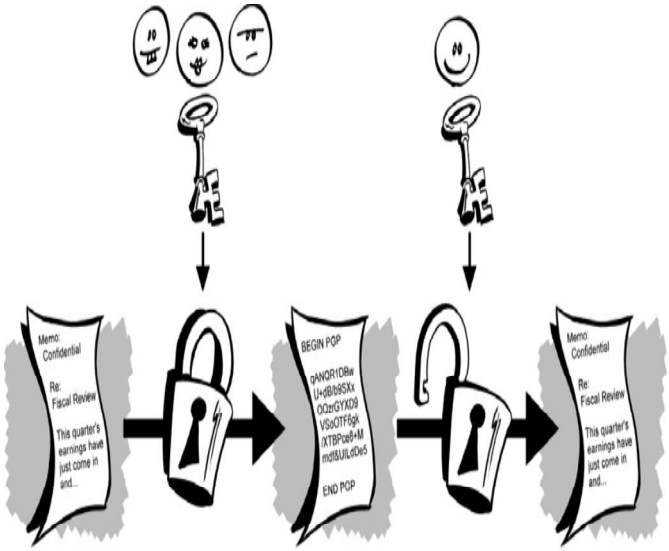

Fig 2. ASSYMETRIC CRYPTOGRAPHY

THE ADVANTAGES OF PUBLIC-KEY CRYPTOGRAPHY COMPARE WITH SECRET-KEY CRYPTOGRAPHY:

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel), and there may be a chance that an enemy can discover the secret keys during their transmission. Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos secret-key authentication system involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. Public-key authentication, on the other hand, prevents this type of repudiation; each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation. The primary advantage of public-key cryptography is increased security and convenience: private keys never need to transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel), and there may be a chance that an enemy can discover the secret keys during their transmission. Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos secret-key authentication system involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. Public-key authentication, on the other hand, prevents this type of repudiation; each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation.

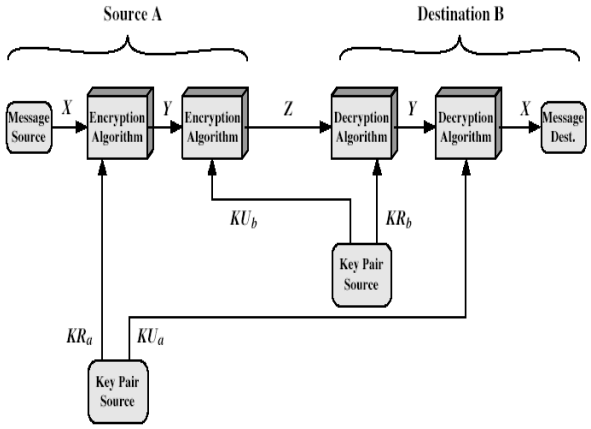

Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

Fig 3. PUBLIC KEY AUTHENTICATION

.The most obvious application of a public key encryption system is confidentiality. A message that a sender encrypts using the recipient's public key can be decrypted only by the recipient's paired private key. This assumes, of course, that no flaw is discovered in the basic algorithm used. Another type of application in public-key cryptography is that of digital signature schemes. Digital signature schemes can be used for sender authentication and non repudiation. In such a scheme, a user who wants to send a message computes a digital signature for this message, and then sends this digital signature (together with the message) to the intended receiver.

❖ ALGORITHM FOR CRYPTOGRAPHY:

RSA is a cryptosystem, which is known as one of the first practicable 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. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman

OPERATION:

1.Choose two distinct prime numbers *p* and *q*. For security purposes, the integers *p* and *q* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2.Compute $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3.Compute $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$ where ϕ is Euler's totient function.

4.Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; i.e., e and $\phi(n)$ are coprime. e is released as the public key exponent.e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

5.Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\phi(n)$).This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\phi(n)}$This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and $\varphi(n)$, respectively.d is kept as the private key exponent.We can be compute the encryption by using the formula $c \equiv m^e \pmod{n}$,and the decryption by using C = c^e(MOD n). Given m, she can recover the original message M by reversing the padding scheme.

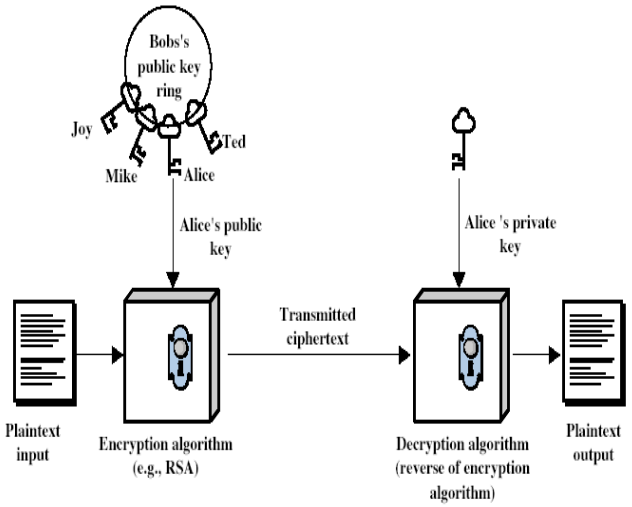

Fig 5.ENCRYPTION AND DECEYPTION WITH RSA

Suppose Alice uses Bob's public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message. Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and

attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice's public key. He raises the signature to the power of *e* (modulo *n*) (as he does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of the message was in possession of Alice's private key, and that the message has not been tampered with since.

CONCLUSION:

With the introduction of computer, the need for automated tools for protecting files & other information stored on the computer, to protect these type of files & our network I use cryptography**.** In this paper, I can elaborate the Secret key and public key. Also the RSA algorithm is explained by me for the strong security purpose of system. With the future scope, we can elaborate more algorithms with RSA for strong security purpose.

REFERENCES:

1. X. Wu, P. D. Le, and B. Srinivasan, "Security Architecture for Sensitive Information System" , Convergence and Hybrid Information Technologies, pp. 239-266, March 2010.

2. S. A. Hameed, H. Yuchoh, and W. F. Al-khateeb, "A model for ensuring Data Confidentiality in Healthcare and Medical Emergency", IEEE 4th International Conference on Mechatronics, pp. 1-5,2011.

3. C. Mockel, 'Usability and Security in EU E-Banking System," IEEE/IPSJ 11th International Symposium on Application and the Internet, pp.230-233,2011.

4. A. J. Menezes P. C. van Oorschot; S. A. Vanstone (1997). *Handbook of Applied Cryptography*. ISBN 0-8493-8523-7.