Abstract - The Research was undertaken in order to develop better and faster algorithms for implementation of RSA system in Cryptography. Various types of Symmetrical and Asymmetrical Cryptography methods were studied. Faster implementations of public-key cryptography, and in particular of RSA are of utmost importance nowadays. Computer security is becoming increasingly important to companies and organizations all over the world. Computers are being used for communications between companies that may be in different cities or even different countries. So in this paper we secure our textual data with RSA cryptography using MATLAB.

Keywords –RSA, Text Encryption, Decryption, Public Key, Private Key, Cryptography, Matlab.

I. INTRODUCTION

Generally speaking, cryptography falls into two main categories: secret and public key cryptography. Secret-key cryptography is based on a prior exchange of a common secret key. Since a single key is used for both encryption and decryption, the major issue associated with symmetric-key systems is the key distribution problem that is an efficient method has to be devised for the parties to agree upon and then exchange keys securely. In 1970, W. Diffie and M. E. Hellman proposed an efficient method of exchanging a shared secret key over an unsecured communications channel and thus setting up the basis of a new type of cryptography: the public-key cryptography. The assymetric-key cryptography uses a key (public) for encryption, which is made available to everyone at the sending end, and another one (secret) for decryption that is known only by the recipient of the message. In 1977, R. Rivest, A. Shamir, and L. Adleman introduced the RSA cryptosystem which became the most widely used public-key cyptosystem in the world. Its security depends upon the intractability of the integer factorization problem and it can be used to provide both data encryption and digital signatures. In what follows the RSA encryption-decryption protocol is shortly reviewed.

II. BACKGROUND

The RSA algorithm is named after the 3 MIT researchers that developed it in 1978. (Ronald Rivest, Adi Shamir e Leonard Adleman). The cryptographic telephone applications developed by Kryptotel use this algorithm together with the AES to enable the encryption on the Iphone, the fixed telephone and for the applications that are installed on the PC. With the development of electronic devices (smartphone, smart card, token and PC) the application of the algorithm has become of vital importance to guarantee secrecy, authentication and protection of the information that goes through or that is stored in the devices. The disadvantage of using a private key algorithm (symmetric cryptography) is that it involves the use of only one encryption and decryption key. In order to be used the key has to be exchanged between the sender and the recipient and it is during this exchange that the Key can be intercepted. In 1976 two cryptologists, Diffie and Hellman, were inspired by the limitations that symmetric algorithms had, and they introduced a new approach to cryptography, by assuming that the only way to overcome the limitations was by using two distinct keys for the data encryption and decryption. The advantage is that the decrypting key, also called private key, can be sent using insecure communication methods while the private key used for the encryption operations is safely stored by its owner.
Many attempts were made to create an algorithm that would succeed by following this theory. The first algorithm that was able to embrace this approach was discovered in 1978, and it was exactly the RSA, the most used and efficient algorithm used to this day. The RSA cipher represented a real turning point for practical applications with high quality, guaranteed security and reliability. In fact the expression strong encryption was invented exactly with the RSA algorithm.

II. Overview of Encryption and Public-Key Cryptosystems

Modern cryptosystems are typically classified as either public-key or private-key. Private-key encryption methods, such as the Data Encryption Standard (DES), use the same key to both encrypt and decrypt data. The key must be known only to the parties who are authorized to encrypt and decrypt a particular message. Public-key cryptosystems, on the other hand, use different keys to encrypt and decrypt data. The public-key is globally available. The private-key is kept confidential.

The Key Distribution Problem

Private-key systems suffer from the key distribution problem. In order for a secure communication to occur, the key must first be securely sent to the other party. An unsecure channel such as a data network cannot be used. Couriers or other secure means are typically used. Public-key systems do not suffer from this problem because of their use of two different keys. Messages are encrypted with a public key and decrypted with a private key. No keys need to be distributed for a secure communication to occur.

A. Public-Key Cryptosystems

A user wishing to exchange encrypted messages using a public-key cryptosystem would place their public encryption procedure, E, in a public file. The user's corresponding decryption procedure, D, is kept confidential.

Rivest, Shamir, and Adleman provide four properties that the encryption and decryption procedures have:

Deciphering the enciphered form of a message M yields M. That is, D(E(M)) = M

E and D are easy to compute.

Publicly revealing E does not reveal an easy way to compute D. As such, only the user can decrypt messages which were encrypted with E. Likewise, only the user can compute D efficiently.

Deciphering a message M and then enciphering it results in M. That is, E(D(M)) = M

As Rivest, Shamir, and Adleman point out, if a procedure satisfying property (3) is used, it is extremely impractical for another user to try to decipher the message by trying all possible messages until they find one such that E(M) = C. A function satisfying properties (1) - (3) is called a "trap-door one-way function". It is called "one-way" because it is easy to compute in one direction but not the other. It is called "trap-door" because the inverse functions are easy to compute once certain private, "trap-door" information is known.

A.1 The Public-Key Cryptosystem Encryption and Decryption Process

Suppose user A wants to send a private message, M, to user B.

User A gets User B’s public key from some public source.
User A encrypts message M using B’s public key. This produces a ciphertext message, C
Ciphertext message C is sent over some communication channel
Upon receipt, user B decrypts message C using their private key. This results in the original message M.

B. Digital Signatures
Property of public-key cryptosystems allows a user to digitally "sign" a message they send. This digital signature provides proof that the message originated from the designated sender. In order to be effective, digital signature need to be both message-dependent as well as signer-dependent. This would prevent electronic "cutting and pasting" as well as modification of the original message by the recipient.

Suppose user A wanted to send a "digitally-signed" message, M, to user B:

User A applies their decryption procedure to M. This results in ciphertext C.
User A applies the encryption procedure of user B to C. This results in message S.
Ciphertext message S is sent over some communication channel
Upon receipt, user B applies their decryption procedure to S. This results in ciphertext message C.
User B applies user A's encryption procedure to message C. This results in the original message, M.
User B cannot alter the original message or use the signature with any other message. To do so would require user B to know how to decrypt a message using A's decryption procedure.

III. RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n), the algorithm is as follows:
Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks.
Each block would then be represented by an integer in the same range.
Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
To decrypt ciphertext message C, raise it to another power d modulo n
The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

A. How to Determine Appropriate Values for e, d, and n
Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
Set n equal to p * q.
Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
Find e such that e * d = 1 (mod ((p-1) * (q-1)))
Rivest, Shamir, and Adleman provide efficient algorithms for each required operation.

B. How secure is a communication using RSA?
Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for p and q, the resulting n will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining d without factoring n are equally as difficult.
Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

Features of the RSA algorithm

Following are the main features of the algorithm:
Secrecy and privacy: the content of the information and communication must be ONLY accessible to the sender and the recipient of the information:integrity: the content must not be altered during the exchange phase, therefore it must stay in its original form:authentication: this aspect is very important because RSA guarantees the origin of the sent information, only the sender with his own private key is able to encrypt the message therefore transform the message into an unreadable form consequently the receiver will have confirmation of the origin because he will be able to decrypt the message only through the corresponding public key:repudiation: the sender cannot state that the message has not been encrypted with his private key because the private key used for the encryption is unique and it's the owner's responsibility to make sure that it is not used by non authorized third parties
Practical applications of the RSA algorithm
To this day the RSA together with the AES algorithm is the most used algorithm in commercial systems.
It is used:
- to protect web traffic, in the SSL protocol (Security Socket Layer),
- to guarantee email privacy and authenticity in PGP (Pretty Good Privacy)
- to guarantee remote connection in SSH (Secure Shell).
Furthermore it plays an important role in the modern payment systems through SET protocol (Secure Electronic Transaction).

RSA has been used in most digital data, information and telephone security applications.
The RSA has its advantages of being a reliable and safe system but it also has the disadvantage of being very slow in data calculating. For this reason it is used in hybrid cryptographic systems that simultaneously use symmetric algorithms (AES) for the communication and data encryption phase and public key algorithms (RSA) for the safe delivery of the symmetric key (or session key) that is necessary for encrypting and decrypting the message. There are different levels of encryption in telephone cryptography.

IV. Simulation and Results Discussion
Step 1: Run the rsa.m Matlab code in Matlab software (here Matlab 2015a based simulation used)
Step 2: it ask prime vale for p and q shows in figure 1 & 2:

Note: Take any large prime number for p and q

Step 3: after putting values press enter then it shows calculated public and private keys for RSA in figure 3:
ENCRYPTION AND DECRYPTION OF TEXT DATA WITH RSA CRYPTOGRAPHY USING MATLAB

Step 4: In figure 3: it’s also ask for Enter the message, then we write any text here like “ShipraSahu” see figure 4:

Step 5: now press the enter after writing message it shows the ASCII code of entered message, Ciphertext ASCII message, Decrypted ASCII message and finally shows Decrypted Message as entered message, see figure 5:
V. CONCLUSION

In this paper an algorithm is proposed for RSA a method for implementing a public-key cryptosystem (RSA) using two public keys and some mathematical relation. This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security with normal speed. As a future work multiple file encryption and decryption can be possible. It has broad development prospects. The project application was designed to take the efficiency and reusability into account. Great level of security is achieved using this algorithm. Modified RSA algorithm for file transmission algorithm can be used where high security file transmission required in public forums.

REFERENCES


