International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Asymmetric New Cryptography Algorithm Based on ASCII Code

Yaser M.A. Abualkas[1], Arshed Raad Raheem[2]

[1, 2]Department of Computer Science and Systems Engineering, College of Engineering (A) Visakhapatnam-530003, Andhra University
[1]*319206415031[at]andhrauniversity.edu.in*
[2]*319206415029[at]andhrauniversity.edu.in*

Abstract: ***Encryption is a process of generating secret text from the input text using a secret key and a encryption algorithm. Input text is referred to as plain text and the secret text generated is known as cipher text. Encryption algorithms are mainly divided into two categories which are symmetric key encryption algorithm and asymmetric key encryption algorithm. In Symmetric key encryption algorithm the same key is used by both sender and receiver but in asymmetric key algorithms use different keys for encryption and decryption. The keys are: Private Key and Public Key. The encryption key is public, decryption key is secret. Anyone can encrypt a message but only the one who knows the corresponding private key can decrypt it. The decryption key cannot be derived from the encryption key. Asymmetric key algorithms used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private. In this paper, we present a technique based on asymmetric key encryption algorithm which uses ASCII vales of input text to encrypt the data. Text data encryption techniques are very useful in data communication where one user want to send some secret messages to another users.***

Keywords: Encryption, Decryption, ASCII con, Symmetric Encryption, Plain Text, Cipher Text, Cryptography, Diffie-Hellman , RSA, ElGamal, ECC, DSA

1. Introduction

Asymmetric key algorithms are used for key distribution. Asymmetric key algorithms are also known as public key algorithms. Asymmetric key algorithms using two keys: A public key and a private key. Public key are used to encrypt the message and private keys are used to decrypt the message. Public key is known to public and private key is only known to user. So there is no need to distribute the keys before transmission [1]. In this type of algorithms it is very difficult to derive one key from the other.

Asymmetric encryption is also know Public-Key Encryption Structure Public-key encryption, first publicly proposed by Diffie and Hellman in 1976 [2], is the first truly revolutionary advance in encryption in literally thousands of years. Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns, such as are used in symmetric encryption algorithms. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

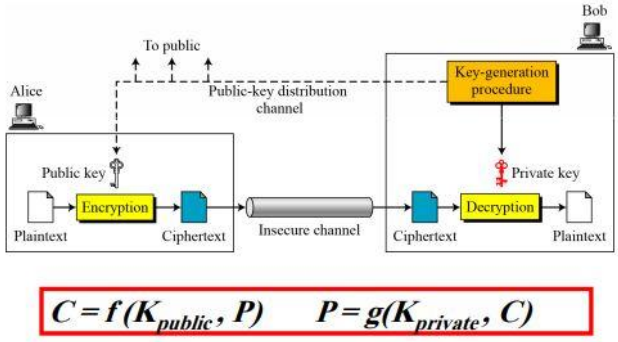

Figure 1: Asymmetric encryption scheme

A public-key encryption scheme has six ingredients

1) Plaintext: This is the readable message or data that is fed into the algorithm as input.
2) Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
3) Public and private key: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact
4) Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
5) Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

As the names suggest, the public key of the pair is made public for others to use, while the private key is known only to its owner. A general-purpose public-key cryptographic algorithm relies on one key for encryption and a different but related key for decryption.

The essential steps are the following:

1) Each user generates a pair of keys to be used for the encryption and decryption of messages.
2) Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others.
3) If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
4) When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

2. Literature Survey

Public-Key Requirements

1) Conditions that these algorithms must fulfill:
   - It is computationally easy for a party B to generate a pair (publickey PUb, private key PRb)
   - It is computationally easy for a sender A, knowing the public key and the message to be encrypted, to generate the corresponding ciphertext
   - It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message
   - It is computationally infeasible for an adversary, knowing the public key, to determine the private key
   - It is computationally infeasible for an adversary, knowing the public key and a ciphertext, to recover the original message
   - The two keys can be applied in either order

2) Need a trap-door one-way function

A one-way function is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible [3]
   - Y = f(X) easy
   - X = f–1(Y) infeasible

3) A trap-door one-way function is a family of invertible functions fk, such that

Y = fk(X) easy, if k and X are known
X = fk –1(Y) easy, if k and Y are known
X = fk –1(Y) infeasible, if Y known but k not known

4) A practical public-key scheme depends on a suitable trap-door one-way function.

Public-Key Cryptosystem: Authentication and Secrecy

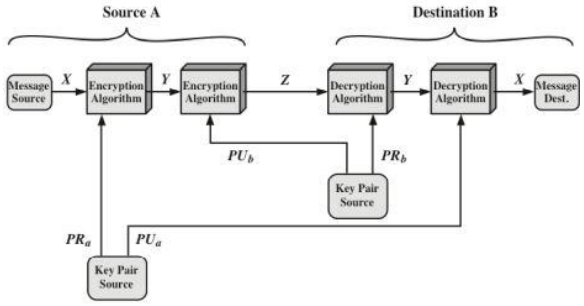

Figure 2: Authentication and Secrecy

3. Related Work

Several works have been done to develop a new cryptographic algorithm for a higher level of security. A new symmetric cryptographic algorithm based on ASCII code using random number techniques was proposed early by Yaser M A Abualkas [4] to improve the time and speed for encryption and decryption of data of end-to-end delay and to provide higher level of security [5]. Day by day the level of security is going to be higher. Still now many researchers are working on cryptography and data hiding. A new cryptographic algorithm for the Real Time Application was in [6] to improve the time for encryption and decryption of data of end-to-end delay and to provide higher level of security. A cryptographic algorithm based on ASCII conversion and a cyclic mathematical function was presented in [7]. A user of RSA creates and then publishes a public key based on two larges prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly [8]. Some researchers have developed a new cryptosystem using multiple cryptographic assumptions which offers a greater security level than that schemes based on a single cryptographic assumption [9]. Blowfish is a symmetric key block cipher, designed in 1993 by B. Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications [10]. A basic study on cryptography which is a solution for information security threats has been shown in [11]. In this paper, a new cryptographic algorithm is proposed which involves ASCII, number system conversions, matrix manipulation and the usage of cyclic mathematical used in [7].

4. Proposed Work

4.1 Introduction

The main focus of the proposed system is to standardize the algorithm proposed in paper [4] in order to make it more complex and make the text unpredictable. We are enhancing the algorithm proposed in paper [4], i.e., we are encrypting the data by change the techniques from symmetric to asymmetric encryption and decryption algorithm. In this research paper is to propose a new technique of asymmetric encryption based on ASCII code. It changes the data into its respective ASCII values and then converts these ASCII values to cipher text using public key. The method also uses mathematical operation to produce final cipher text which makes data more secure from getting decrypt by intruders. At the receiver side decrypted data by private key of the sender. The main idea behind asymmetric-key cryptography is the concept of the trapdoor one-way function and we using the RSA algorithm rule to produce secret message.

Features of RSA algorithm

One-Way Function (OWF)
1) f is easy to compute y=f(x)
2) f is difficult to compute x=f (y)
   Trapdoor One-Way Function (TOWF)
3) Given y and a trapdoor, x can be computed easiy

RSA Cryptosystem

The most common public-key algorithm is the RSA cryptosystem, cryptosystem, named for its inventors (Rivest, (Rivest, Shamir, Shamir, and Adleman) Adleman).

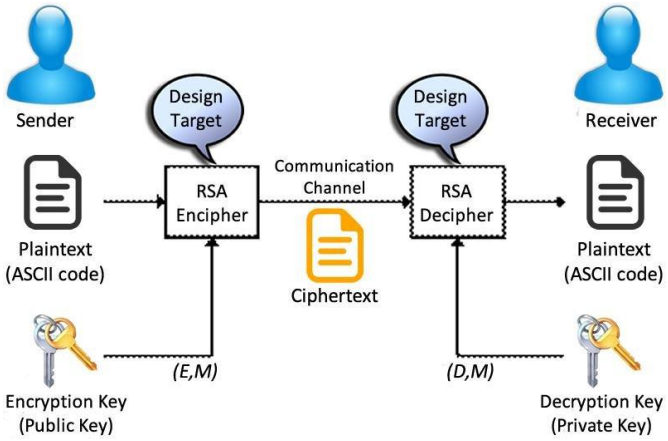

Figure 3: RSA cryptosystem

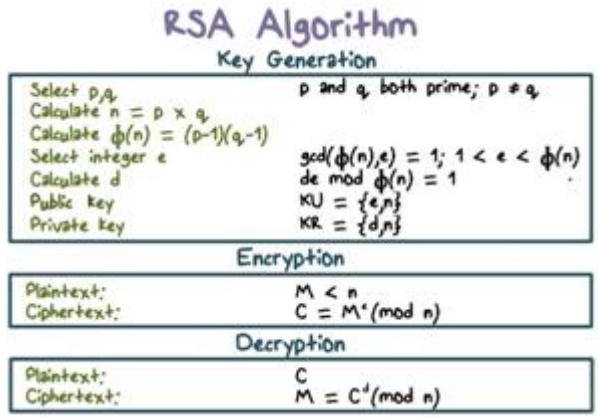

Figure 4: RSA key generation, Encryption and Decryption

Why is RSA Secure? [3]

The real promise behind RSA's security is

The assumption that factoring a big number is hard and the best knowing factoring methods are really slow:

- To factor a 512-bit number with the best known techniques would take about 30,000 MIPS-years.
- MIPS-year=# of steps processed for one year at one million instructions per second=31.5 trillion instructions.

Encryption Phase:

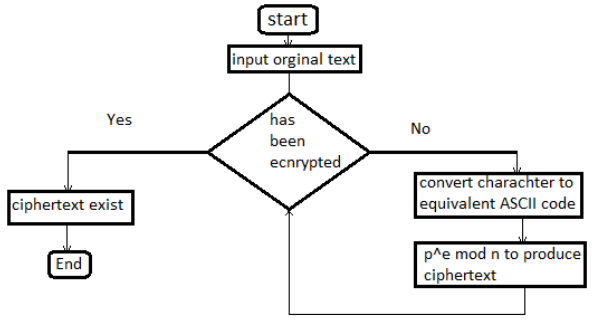

Figure 5: Flowchart of the Encryption Algorithm

In encryption phase of proposed algorithm, at first to write a sequence of character to convert it to equivalent ASCII code and the value of ASCCI code to the equation to produce ciphertext in forms of c^e mod n.

Example:

Bob chooses 7 and 11 as p and q and calculates n = 77. The value of φ(n) = (7 − 1)(11 − 1) or 60. Now he chooses two exponents, e and d, from Z60 ∗. If he chooses e to be 13, then d is 37. Note that e × d mod 60 = 1 (they are inverses of each Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5.

Plaintext p=5

e= 13

c=p^e mod n

c=5^13 mod77=26

Ciphertext c=26

Semi code of Encryption:

```
Encryption(p,e,n){
c=Math.pow(p, e)mod n;
//where p is ASCII value
}
```

Decryption Phase:

In the decryption phase of the proposed algorithm, at first will compare the cipher text with plain text if it equal, print the plain text, if not apply decryption algorithm , ciphertext value taken to decrypt it by using the value of ciphertext cexponentialy value of d modular n to get plaintext.

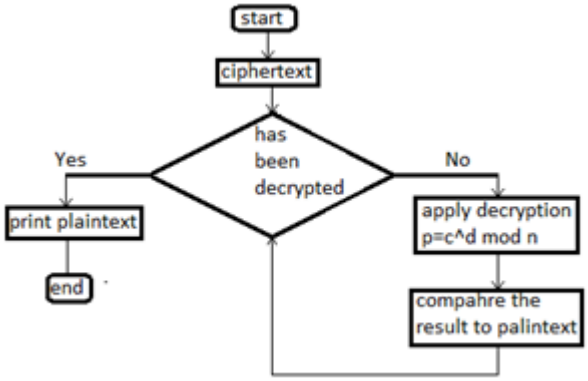

Figure 6: Flowchart of the Encryption Algorithm

Example:

Regarding to previous example we got chiphertext value equal to 26, applying decryption algorithm to obtain plaintext from chipertext.

Ciphertext c = 26

d=37

p=c^d mod n

p=26^37 mod 77= 5

Plaintext p= 5

Semi code od Decryption:

```
Decryption(c,d,n){
p=Math.pow(c, d) mod n;
//where c is ciphertext
}
```

5. Result

The result from the algorithm is very efficient with faster processing. A sample scenario of result of the developed algorithm implemented by Java programming language is explained here. Fig. 5 shows the plaintext to be encrypted though the algorithm. Applying the encryption algorithm the ciphertext of unprintable characters is shown in Fig. 6.

6. Conclusion

Symmetric-key cryptography is based on personal secrecy in this paper presented a new Asymmetric cryptography algorithm based on ASSCI code. The proposed algorithm can be used to encrypt and decrypt text messages based on the ASCII code of characters in most sensitive data and critical position like bank account details, messages..etc. The main idea of the proposed algorithm is to ensure higher security and to hide data in effective way. In future, we increase the security technique and extending the proposed idea to work for asymmetric cryptography as well.

References

[1] Dr. Prerna Mahajan, Abhishek Sachdeva, 2013 , A study of Encryption algorithms AES, DES and RSA for security, Global Journal of Computer Science and Technology, Volume 13 Issue 15 Version 1.0
[2] Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp. 644-654.
[3] Haipeng Dai haipengdai@nju.edu.cn 313 CS Building ,Department of Computer Science and Technology, Nanjing University
[4] Yaser M A Abualkas, A New Cryptography Algorithm Based on ASCII Code ,April 2021, Mtech CST department, Andhra university.
[5] A. H. Omari, B. M. Al-Kasasbeh, R. E. Al-Qutaish, and M. I. Muhairat, “A New Cryptographic Algorithm for the Real Time Applications”, Proc. of the 7th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP), pp. 33-38, 2008
[6] A. H. Omari, B. M. Al-Kasasbeh, R. E. Al-Qutaish, and M. I. Muhairat, “A New Cryptographic Algorithm for the Real Time Applications,” Proc. of the 7th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP), pp. 33-38, 2008.
[7] M. P. Uddin, M. A. Marjan, N. B. Sadia and M. R. Islam, “Developing an Efficient Algorithm to Combine Cryptography and Steganography Based on ASCII Conversions and Cyclic Mathematical Function,” 3rd IEEE International Conference on Informatics, Electronics & Vision, May 23-24, 2014.
[8] R. Rivest, A. Shamir, L. Adlemanm, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
[9] E.S. Ismail and M.S. Hijazi, “New Cryptosystem Using Multiple Cryptographic Assumptions,” Journal of Computer Science, vol. 7, no.12, pp. 1765-1769, 2011.
[10] Dahna and McConnachie, "Bruce Almighty: Schneier preaches security to Linux faithful," Computerworld. p. 3.
[11] M. V. Kumar, “Cryptography–A solution for information security Threats,” Golden Research Thoughts, vol. 2, no.1, 2013