# RSA Asymmetric Cryptosystem beyond Homogeneous Transformation

**Prince Oghenekaro Asagba, Enoch O. Nwachukwu**
**Department of Computer Science, University of Port Harcourt, PMB 5323, Port Harcourt, Rivers State, Nigeria (pasagba@yahoo.com),**

## Abstract

*The Internet is an insecure open network and its use and connectivity have witnessed a significant growth, and this has made it vulnerable to all forms of attacks. A threat to a network can cause harm or interrupt the network. In this paper, we looked at the security of data and message, using asymmetric cryptography, with regard to secret communication over an insecure network. Rivest, Shamir, and Adleman (RSA), is an asymmetric cryptosystem. Our work is an extension and modification of the RSA cryptosystem. What is actually being sent across the insecure network is the encrypted data. In carrying out this research, the methodology we have adopted is the Structured Systems Analysis Method (SSADM). RSA is based on homogeneous encryption, which means that the message to be encrypted does not undergo any form of transformation or encoding prior to encryption and the level of encryption is one. In our work, we extended the level of encryption to two, which makes it heterogeneous. Prior to encryption, the message is subjected to an encoding mechanism using 'Delta Encoding Technique'. We developed a number of programs for: prime number generation, pre-computation of public and private keys, and privacy, using Turbo C++ 4.5. Our work was able to address up to 32 bits. The objective of this paper is to develop an encryption scheme which is heterogeneous compared with the current RSA system that is homogeneous, which brings us toward improved RSA cryptosystem for privacy in terms of the level of transformation.*

**Keywords:** Cryptosystem, Internet Security, Encryption, Decryption, Homogeneous, Heterogeneous

---

### 1.0 Introduction

Security is a system of safeguards designed to protect a computer system and data from deliberate or accidental damage or access by unauthorized persons [4]. Security of information is not a new phenomenon. It is as old as civilization. Security of information was born out of the consciousness to have private transmission. The first communication channels were based on trustworthy messengers. The security of the communication channels rely strictly on the messengers. With the advent of computers and computer networks, the issue of security became more prominent because the communications channels are vulnerable and subject to attack by intruders since it involves open communication traffic. A network, or communications network, is a system of interconnected computers, telephones, or other commutations devices that can communicate with one another and share applications and data [7]. A computer network is a collection of communicating computers and the communicating media connecting them [13]. The Internet is an insecure open network.

Security is a broad topic that ranks almost first in a computer networked environment [1]. The only system that is truly secure is the one that is switched off and unplugged [11]. A system is secure if it adequately protects information that it processes against unauthorized disclosure, unauthorized modification, and unauthorized withholding (also called denial of service) [9]. In today's heavily networked environment, we must guard against both obvious and subtle intrusions that can delete or corrupt vital data [8] by using appropriate encryption technologies.

Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over untrusted medium like the Internet [3].

Cryptosystems is considered to be the collection of encryption and decryption systems, the key generator, as well as the protocols for key transmission [12]. The term cryptosystems is used to describe cryptographic algorithms and their characteristics.

The introduction of public-key cryptography by Diffie and Hellman in 1976 was an important watershed in the history of cryptography. The work sparked off interest in the cryptographic research community and soon several public-key schemes were proposed and implemented. The RSA, being the first realisation of this abstract model, is the most widely used public-key scheme today [2]**.** The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem [10]. RSA is an asymmetric cryptosystem. Asymmetric cryptosystems involves two keys - a private key and a public key that are mathematically related. A message encrypted with one key can be decrypted only with the other. It is extremely difficult to determine the value of one key by examining the other. Usually, two large primes are selected to compute the keys.

If any of the two prime factors of a participant's public RSA-modulus can be found, then the private key of that participant can be found, and the system is considered to be broken. If the primes are properly chosen (that is large enough), then finding them given only their product (the RSA-modulus) is believed to be a computationally infeasible task. To make the system secure, the primes chosen must be sufficiently large. On the other hand, large primes imply a large RSA-modulus, which leads to substantial computational overhead when using the RSA system. Thus, in RSA there is a trade-off between security and efficiency: on the one hand, moduli must be large for security; on the other hand, small moduli are preferred for efficiency. How large they have to be, depends on the speed of so-called factorization algorithm [5]. In this paper, we focused on privacy and secrecy only. In our work, we extended the level of encryption to two, which makes it heterogeneous. Prior to encryption, the message is subjected to an encoding mechanism using 'Delta Encoding Technique'. The objective of this paper is to develop an encryption scheme which is heterogeneous compared with the current RSA system that is homogeneous.

## 2.0 Problem Statement

When a message is sent across an insecure network, it is most likely to pass through a number of machines on the way. Any of these machines is capable of reading and recording the message for future use, and this do not portray privacy. In reality, people would prefer to have their message(s) concealed, so that they should be able to send a message that can only be read by the intended recipient. The quest for privacy has motivated researchers to adopt the techniques of cryptography in sending secure message(s), which RSA addresses. RSA tries to proffer solutions using cryptography based on the following: homogenous transformation, block cipher, and deterministic encryption scheme.

Many steps can be taken to prevent unauthorized access to organizational data and

networks, but no network is completely safe [6]. The issue of homogenous transformation, block cipher, and deterministic encryption comes into focus. In existing open networks, such as the RSA, there are security problems associated with secret communication and digital signature. Threats and attacks may occur as a result of communications over an open insecure network. The problem of security on an open network like the Internet has been of much concern to the society. This paper looked at RSA's homogenous transformation.

## 3.0 Materials and Method

We developed a number of programs for: prime number generation, pre-computation of public and private keys, and privacy, using Turbo C++ 4.5. The capacity of the compiler and computer is less than 32 bits and could not address or accept values above $2^{32}$ for p and q respectively. Our work was able to address up to 32 bits.

Looking from a software engineering perspective, a number of design methodologies suitable for asymmetric cryptosystems have been put forward. They include modern structured design, Structured Systems Analysis Method (SSAM), Prototyping, Object-oriented Design, Rapid Application Development (RAD), Joint Application Development (JAD), and Structured Systems Analysis and Design Methodology (SSADM). The methodology we have adopted in our research is the structured systems analysis method.

### Present Procedure of RSA

We looked at the existing procedure of RSA asymmetric cryptosystems. The present RSA procedure follows or adopts homogeneous encryption approach.

### Homogeneous Encryption

Prior to encryption, the message m is prepared to an integer form before encryption takes place using:

$$c = m^e \bmod n$$

Where:

c is the ciphertext, m is the message, e is the public key, and n is the modulus.

We can describe such encryption as homogeneous since the level of encryption is one.

### Heterogeneous Encryption

After the message m has been prepared to an integer form, it undergoes a form of transformation or encoding before encryption commences. This type of encryption can be described as heterogeneous since the level of encryption or transformation exceeds one.

$$\mathbf{c = F^e \bmod n}$$

Where:

c is the ciphertext based on F, F is the transformed message, e is public key, n is modulus.

### 3.1 RSA Algorithms for Secret Communication of the Existing RSA System

RSA algorithms for privacy for the existing system include: algorithm for key generation and algorithm for asymmetric encryption.

- **Algorithm for Key Generation**

If communication must exist between two entities, each entity must be capable of creating an RSA public key and a related private key. Entity X does the following:

(a) Generate any two large prime numbers, p and q having approximately the same size.

(b) Compute n = pq and z = (p-1) (q-1).

(c) Compute public key, e, by choosing any number that is relatively prime with z such that e has no common factors with z.

(d) Compute private key, d, by solving the equation:

e x d = 1 (mod z).

That is, e x d is the smallest elements in the series z+1, 2z+1, 3z+1, etc., that is divisible by z.

(e) X's public key is (n, e) and X's private key is d. e, d are the encryption and decryption exponents, n is the modulus.

- **Algorithm for RSA Asymmetric Encryption**

Entity Y encrypts a plaintext m meant for X, and X decrypts it. Y does the following:

**(a) Encryption:**

1. Get X's public key, (n, e).

2. Prepare the message in the form of an integer m in the interval, [0, n-1].
3. Compute $c = m^e \bmod n$.
4. Send encrypted text or cipher text c to X.

**(b) Decryption:**

X uses the private key, d, to compute:

$m = c^d \bmod n$ (to recover message m).

Where:

m is the original Message/Plaintext.

c is the Cipher text/ encrypted text.

e is the Encryption key.

d is the Decryption key.

n is the RSA modulus.

### 3.2 Data Flow Diagram (DFD) of the Existing RSA System

A top level Data Flow Diagram (DFD) for RSA algorithm for secret communication (privacy /encryption) is shown in Figure 1.

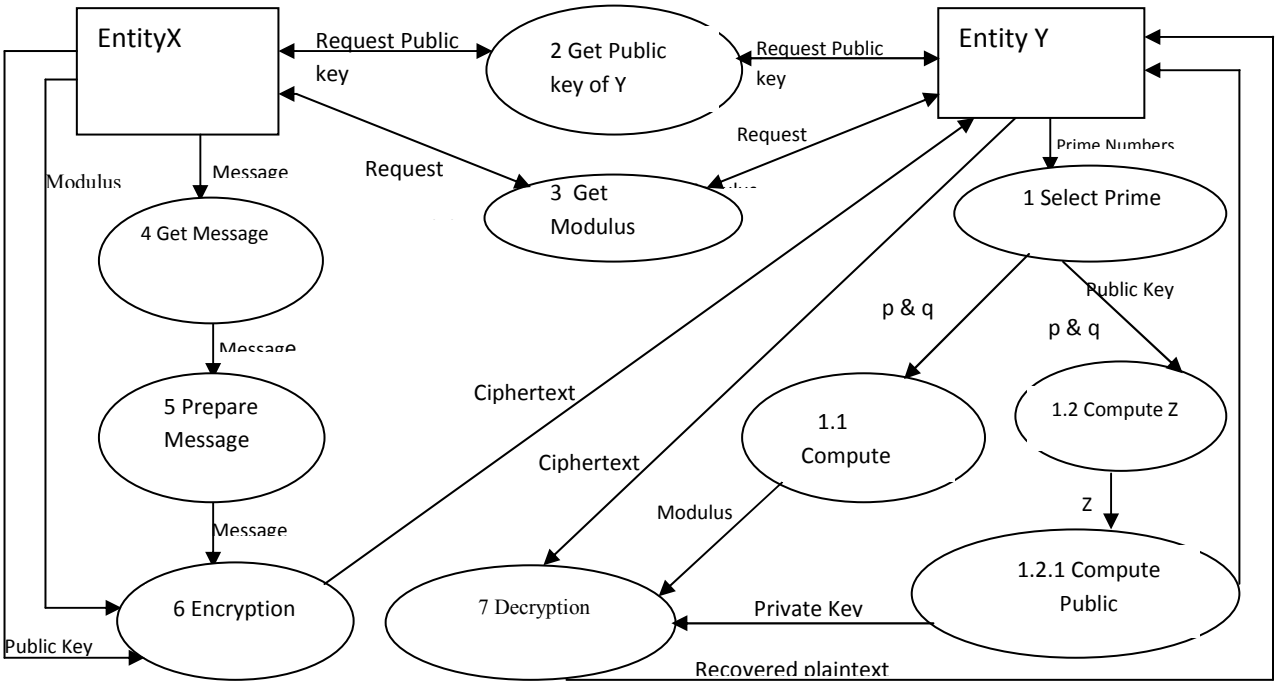


**Fig. 1: A top level DFD for RSA encryption**

### 3.2 Our Proposed RSA Algorithm for Privacy

Our proposed algorithms for privacy include: key generation and asymmetric encryption. The key generation is the same as in existing secret communication.

- **Algorithm for Asymmetric Encryption**

Entity Y proceeds as follows:

a) Enter message.

b) ASCII of message

c) Encode message using Delta encoding (F) - Newton Forward Differential Technique.

d) Input seed for the generation of random characters.

e) Encryption: using the encoded data, F

$c = F^e \bmod n$

Where:

c = Ciphertext based on F

e = Public key

n = Modulus

f) **Decryption:**

$F = c^d \bmod n$

Where:

F = Decipher text based on c

d = private key

n = modulus

Encode F using Delta encoding - Newton Backward Differential technique to recover m.

### 3.4 Data Flow Diagram (DFD) of the Proposed RSA Algorithms

A top level Data Flow Diagram of our proposed RSA algorithm for secret communication (privacy) is shown in Figure 2.

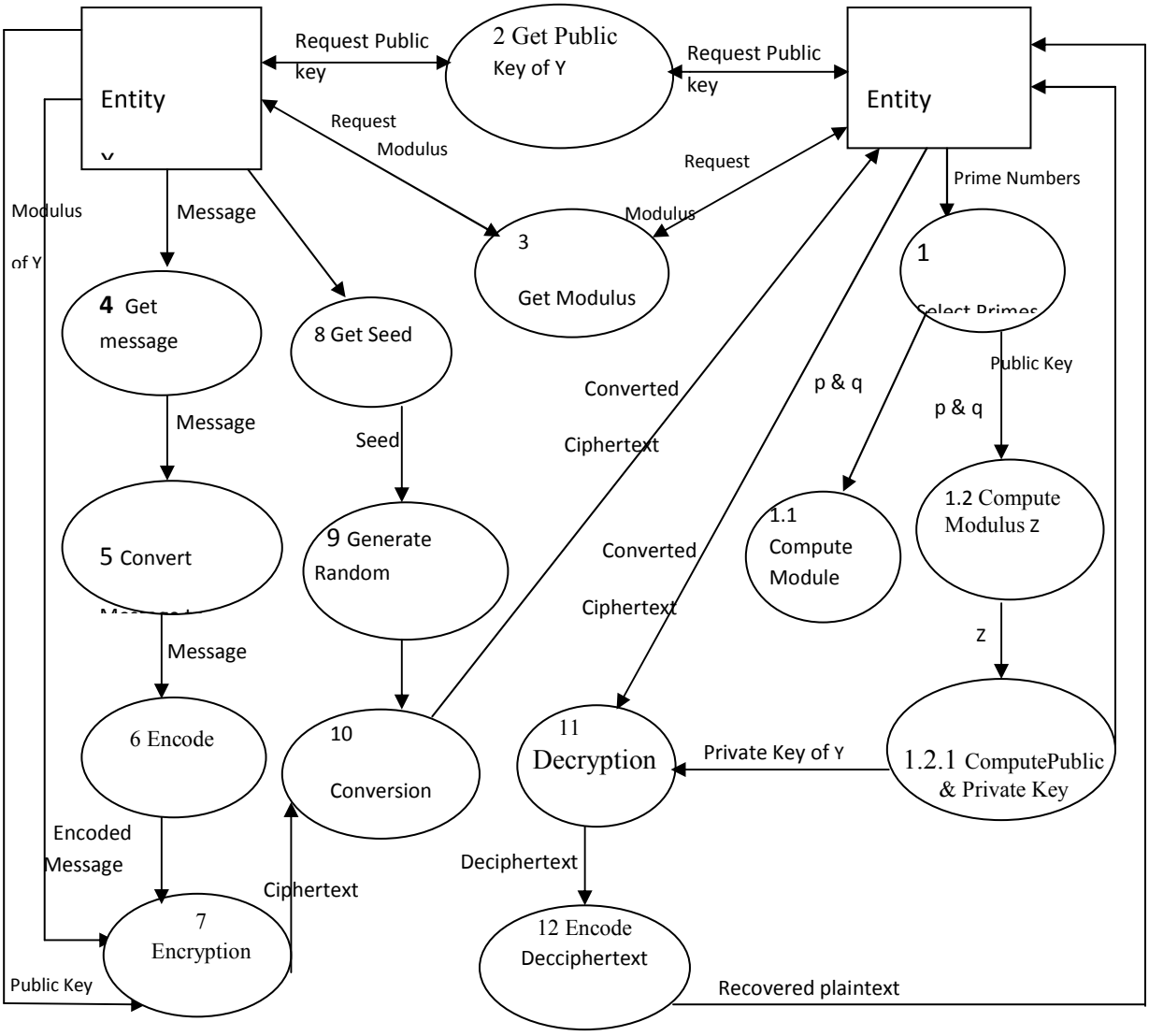


**Fig. 2: A top level data flow diagram of our proposed RSA algorithm for**

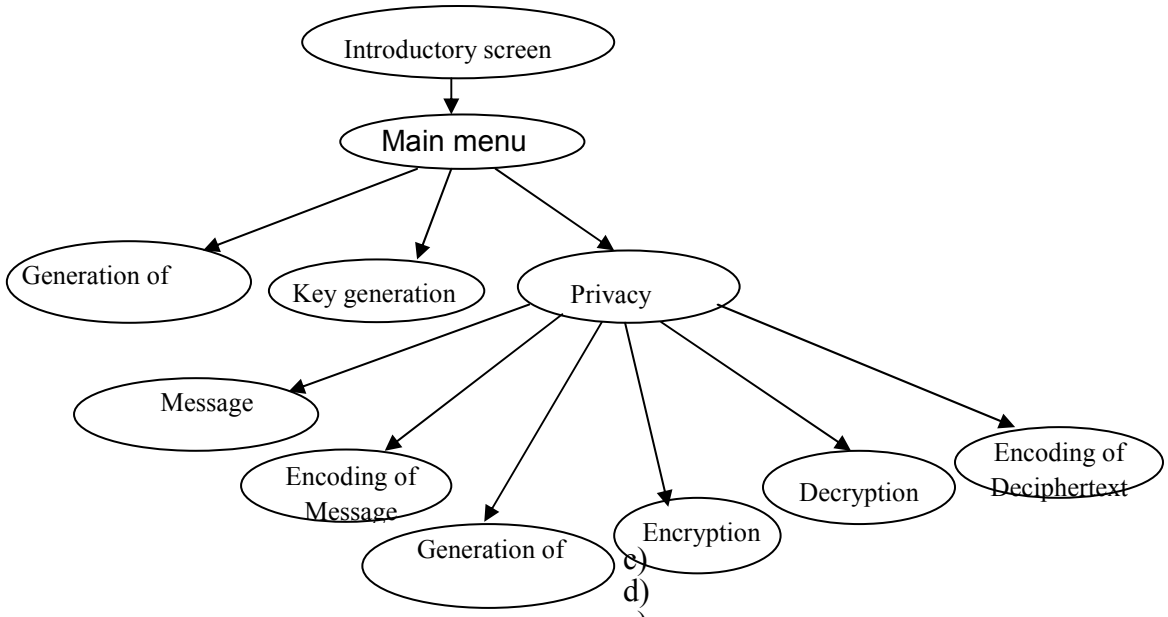


**Fig. 3: A Schematic diagram of the various modules in our proposed RSA encryption**

### 3.5 Design Specification

The design of encryption schemes is presented.

**Design of Cryptographic Algorithm**

To design an encryption scheme irrespective of its type - symmetric or asymmetric requires one to select:

1) a message space m,
2) a ciphertext space c,
3) a key space k,
4) a set of encryption transformation $e_k$: m c and
5) a corresponding set of decryption transformation $d_k$: c m

**Prime Number Generation and Selection of Prime**

Prime numbers are generated prior to encryption for p and q. The prime p and q are selected in such a way that when n = pq is factored, the result will be computationally infeasible. Some basic restrictions on the primes are:

a) p and q should be about the same bitlength, and very large.
b) b) p - q should not be the too small. If p - q is small, then p ≈ q and hence p ≈ √n. Thus, n
c)
d)
e)
f)
g)
h)
i)
j)
k)
l)

could be factored efficiently simply by trial division by all odd integers close to √n. If p and q are chosen at random, then

m) p - q will be appropriately large with Overwhelming probability [10].

In this paper, our values for p and q were not necessarily large perhaps because of the compiler used in the research. What we did is subjecting the message to be encrypted to an encoding mechanism prior to encryption.

**Input / Output Specifications**

The input specifications are the prime numbers p and q used to generate keys, public and private keys, respectively, and the data/message to be encrypted. The output specifications are the encrypted data/message and the decrypted message.

### 4.0 Delta Encoding Techniques

We used the Delta Encoding Scheme, Newton Forward and Backward Differentials to represent a change in a code or object. Data are recorded as difference between successive objects or characters, which attest to the fact

that data are disguised in some way. The first value in this scheme is always the same as the original message or data stream. The delta portrays a difference (F) between the corresponding values. For example, an illustration of original input values and encoded form is shown in Table 1.

**Table 1: Illustration of Original Input Values and Encoded Form**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Original value** | 15 | 22 | 4 | 7 | 9 | 3 |
| **Encoded form** | 15 | 7 | -18 | 3 | 2 | -6 |

### 4.1 Newton Forward Differential

Newton forward differential is represented as:

$\mathbf{F_d = m_d}$ (for the first value of m)

For subsequent values of m, we have

$$\mathbf{F_{d+1} = m_{d+1} - m_d}$$

Where:

d = 1, 2, 3, … p, m is the message space, p is the data stream .

### 4.2 Newton Backward Differential

Newton backward differential is represented as:

$\mathbf{m_d = F_d}$ (for the first value of original F)

For subsequent values of F, we have

$$\mathbf{m_{d+1} = F_{d+1} + m_d}$$

Table 2 shows an illustration of RSA algorithm for privacy. If we want to encrypt the message:

WELCOME TO UNIPORT

This corresponds to the 36 digit number 230512031513050020150021140916151820

Note: 23 is the twenty third letter of the alphabet, 05 is the fifth letter of the alphabet, and so on. We can encrypt the message with some 2 digits primes instead of 100 digits. To encrypt the message, we break the string up into blocks say 4 digits and compute using modular arithmetic in each block.

$\mathbf{2305^{29} \bmod 3713 = 769}$, and so on.

**Table 2: an lustration of RSA algorithm**

| **Block** | **Ciphertext c** | | **Deciphertext m** |
|---|---|---|---|
| **m** | $\mathbf{m^{29}}$ | $\mathbf{c = m^{29} (\text{mod } 3713)}$ | $\mathbf{m = c^{1361} (\text{mod } 3713)}$ |
| 2305 | $3.291978287^{97}$ | 769 | 2305 |
| 1203 | $2.126685122^{89}$ | 855 | 1203 |
| 1513 | $2.185633169^{92}$ | 2597 | 1513 |
| 0500 | $1.862645149^{78}$ | 1537 | 0500 |
| 2015 | $6.667706333^{95}$ | 2130 | 2015 |
| 0021 | $2.209833471^{38}$ | 2072 | 0021 |
| 1409 | $2.081703154^{91}$ | 0187 | 1409 |
| 1615 | $1.088938301^{93}$ | 1706 | 1615 |
| 1820 | $3.483936667^{94}$ | 1648 | 1820 |

**Illustration of Our New RSA Algorithm for Privacy**

Let us assume that **A** wants to communicate with **B by** sending a **message** to **B** after constructing a pair of keys.

Let us assume that:

A sender chooses:

p = 5, q = 11 and computes:

e = 7, d = 23, n = 55.

Let us assume that the message to protect is "**Web design, and IT.**" Table 3 shows the protected message using Data Encoding Technique.

**Tables 3: A Protected Message Using Data Encoding Technique**

| Message | ASCII value (m) | Delta encoding (F) | Encryption | | Decryption | | Delta encoding | Message |
|---|---|---|---|---|---|---|---|---|
| | | | $F^7$ | $c = F^7 \bmod 55$ | $c^{23}$ | $F = c^{23} \bmod 55$ | | |
| W | 87 | 87 | $3.772547949^{13}$ | 43 | $3.713423473^{37}$ | 32 | 87 | W |
| e | 101 | 14 | 1054113504 | 9 | $8.862933812^{21}$ | 14 | 101 | e |
| b | 98 | -3 | -2187 | -42 | $-2.161392694^{37}$ | -3 | 98 | b |
| | 32 | -66 | $-5.455160701^{12}$ | -11 | $-8.954302433^{23}$ | -11 | 87 | |
| d | 100 | 68 | $6.722988818^{12}$ | 7 | $2.736874734^{19}$ | 13 | 100 | d |
| e | 101 | 1 | 1 | 1 | 1 | 1 | 101 | e |
| s | 115 | 14 | 1054113504 | 9 | $8.86293812^{21}$ | 14 | 115 | s |
| i | 105 | -10 | -10000000 | -10 | $-1.0^{23}$ | -10 | 105 | i |
| g | 103 | -2 | -128 | -18 | $-7.434771361^{28}$ | -2 | 103 | g |
| n | 110 | 7 | 823543 | 28 | $1.92590438^{33}$ | 7 | 110 | n |
| , | 44 | -66 | $-5.455160701^{12}$ | -11 | $-8.954302433^{23}$ | -11 | 99 | , |
| | 32 | -12 | -35831808 | -23 | $-2.0880468^{31}$ | -12 | 87 | |
| a | 97 | 65 | $4.902227891^{12}$ | 10 | $1.0^{23}$ | 10 | 97 | a |
| n | 110 | 13 | 62748517 | 7 | $2.736874734^{19}$ | 13 | 110 | n |
| d | 100 | -10 | -10000000 | -10 | $-1.0^{23}$ | -10 | 100 | d |
| | 32 | -68 | $-6.72288818^{12}$ | -7 | $-2.736874734^{19}$ | -13 | 32 | |
| I | 73 | 41 | $1.947542739^{11}$ | 46 | $1.751580609^{38}$ | 41 | 73 | I |
| T | 84 | 11 | 19487171 | 11 | $8.954302433^{23}$ | 11 | 84 | T |
| . | 46 | -38 | $-1.144155826^{11}$ | -47 | $-2.872438457^{38}$ | -38 | 46 | . |

***Note: In some cases, blank (32) for delta encoding is assigned the value 87 for small letters and for capital letters, blank is assigned the value 32.***

## 5.0 Discussion

RSA is based on block cipher. Our work is based on stream cipher. Stream ciphers are generally faster and more appropriate than block ciphers. Block cipher simultaneously encrypt a collection of characters of a plaintext message using a fixed encryption function. In stream cipher, individual character of a plaintext message is encrypted in turn. Stream ciphers are useful where transmission errors are highly required because they do not propel errors. We evaluated our cryptosystem using a number of messages for encryption and decryption. For the purpose of this paper, we entered a message in our cryptosystem that says: '**Please, let join hands to build our country ourselves. Life is beautiful.'** The ASCII value of the message was computed character-based and later encoded or converted using Newton Forward Differential. The public key, e, and modulus, n, are entered to encrypt the encoded data. Thereafter, the encrypted values are displayed. For decryption, the private key, d, and modulus, n, are entered to decrypt. Finally, the decrypted data are encoded using Newton Backward Differential to recover the text which again is displayed. A sample output is given in Appendix A.

## 6.0 Conclusion and Further Work

In this research, we looked at the security of data or message, using asymmetric cryptography with regard to RSA. Our work is a modification or extension of RSA, which is based on heterogeneous encryption. We developed a number of programs for our cryptosystem. The objective of this paper is to develop an encryption scheme which is heterogeneous compared with the current RSA system that is homogeneous. Our work brings us toward improved RSA cryptosystem through heterogeneous transformation and stream cipher. This research is relevant in secret communication. More work can be done using heterogeneous encryption in the area of digital signature which RSA also addresses.

## References


[1] Adewumi S. E., Garba E. J. D., (2002), Data Security: A Cryptosystems Algorithm Using Data Compression and Systems of Non-Linear Equations, Computer Association of Nigeria Conference Series, Vol.13, pp. 200-221.

[2] Alese, B. K., Philemon E. D., Falaki, S. O. (2012), Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology Vol. 2, No. 9, Sept., pp. 1552 – 1568.

[3] Almarini, A. and Alsahdi, U. (2012), Developing a Cryptosystem for XML Documents, International Journal of Information Science, Vol. 2. No. 5, pp. 65 – 69.

[4] Capron, H. L. (1990), Computers: Tools for an Information Age, The Benjamin/Cummings Publishing Coy. Inc.

[5] De, S. Haldar, A., and Biswas, S. (2013), A Review on Recent Trends in Cryptography, International Journal of Latest Research in Engineering and Computer (IJLREC), Vol.1, Issue 1.Sept- Oct., pp. 50-55.

[6] Fitzgerald, J. and Dennis, A. (1996), Business Communications and Networking, John Wiley and Sons, Inc., 5th ed. USA

[7] Hutchinson, E. S. and Sawyer, C. S. (2000), Computers, Communications, Information: A User's Introduction Comprehensive Version, McGraw-Hill Companies; 7th Ed., USA.

[8] Jajoda , S., Ammana, P. and McCollum , D. C., (1999), Surviving Information Warfare Attacks, IEEE Computer, April, pp. 57-63.

[9] Landwehr, E. C., Heitmeyer, L. C. and Melean , D. J. (2001), A Security Model for Military Message

Systems: Retrospective, IEEE Computer Society, Proceeding of the 17th Annual Computer Security Applications Conference (ACSAC'01).
[10] Menezes, A, Oorschot, P. V. and Vanstone S. (1997), Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC press,
[11] Mufett, A. (1993), Security Fag, Version, 2.2, 1-30 http://nsi.org/library/compsec/fag.htm
O'Leary J. T. and O'Leary, I. L. (1999), Microsoft Internet Explorer 4.0, The McGraw-Hill Companies, USA.
[12] Seberry, J. and Pieprzyk, J. (1989), Cryptography: An Introduction to Computer Security, Prentice Hall of Australia Pty Ltd.
[13] Sullivan , D. R., Lewis, T. G., and Cook, C. R. (1986), Using Computers Today With Applications for the Apple II, Houghton Mifflin Company, Boston, USA.

## APPENDIX A

```
==================P R I V A C Y   P R O G R A M===============

Enter text of message:
============================PLAINTEXT m==== ======================
Please, let us join hands to build our country ourselves. life is beautiful


=======================ASCII VALUE OF TEXT=====================

          P     80
          l    108
          e    101
          a     97
          s    115
          e    101
          ,     44
                32
          l    108
          e    101
          t    116
                32
          u    117
          s    115
                32
          j    106
          o    111
          i    105
          n    110
                32
          h    104
          a     97
          n    110
          d    100
          s    115
                32
          t    116
          o    111
                32
          b     98
          u    117
          i    105
          l    108
          d    100
                32
          o    111
          u    117
          r    114
                32
          c     99
```