www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 19867-19871
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.04

Comparative Study of RSA and Probabilistic Encryption/Decryption Algorithms

N. Priya[1] And Dr. M. Kannan[2]

[1]Reasearch Scholor, MPhil

Department of Computer science, SCSVMV University,

Kancheepuram, Tamilnadu, India

riyams29121@yahoo.com

[2] Asst. Professor

Department of Computer science, SCSVMV University,

Kancheepuram, Tamilnadu, India

saikannan1999@rediffmail.com

Abstract

Networks are virtual windows to the people which allow remote access to geographically distant resources without having to be physically present. This is achieved by sending data back and forth in the network. But networks are vulnerable because of their inherent characteristic of facilitating remote access. Hence network security plays a vital role in real time environment as it protects loss and misuse of the data in the network. There are many applications and algorithms running behind the scene for providing security while transmitting data in the network. One of the most important components of network security is cryptography and it consists of many algorithms that protect user from the adversary like trapdoor, eavesdroppers, hackers etc. There are many well known algorithms which serves this purposes and each have its own advantages and disadvantages. The aim of this paper is to outline the key concepts involved in two algorithms namely Goldwasser-Micali encryption and most widely used RSA. Some of the metrics used for comparison are encryption time, decryption time and size of cipher text with varying plain text sizes which are the key considerations for choosing an encryption algorithm. The comparison of encryption and decryption time with varying cypher text sizes for both the algorithms using math lab code and preliminary observations are depicted in this paper.

Keywords

Goldwasser-Micali encryption, Metirc, Decryption, Algorithms, RSA, Comparison

1. Introduction

Networks are virtual windows to the people which allows remote access to geographically distant resources without having to be physically present by sending data back and forth in the network. Since networks are vulnerable due to their inherent characteristic of facilitating remote access, security to the data being transmitted in the networks is of major concern. Network security plays a vital role in real time environment as it protects loss and misuse of the data in the network. The most important ingredient of network security is cryptography and it consists of many algorithms that protect user from the adversary like trapdoor, eavesdroppers, hackers etc. There are many well known algorithms which serves this purposes and each of them processes its own advantages and disadvantages. The aim of this paper is to outline the key concepts involved in two algorithms namely Goldwasser-Micali (GM) encryption and most widely used Rivest, Shamir, and Adleman algorithm(RSA). This paper introduced the revolutionary idea of public-key cryptography and conjointly provided a brand new and ingenious methodology for key exchange, the safety of that relies on the trait of the separate power downside. Though the researchers had no sensible realization of a public-key secret writing theme at the time, the concept was clear and it generated in depth interest and activity within the scientific discipline community.

In 1978 Rivest, Shamir, and Adleman discovered the primary sensible public-key secret writing and signature theme, currently named as RSA. The RSA theme relies on another onerous mathematical downside, the trait of

resolving massive integers. This application of a tough mathematical downside to cryptography revitalized efforts to seek out additional economical strategies to issue. Nineteen Eighties saw major advances during this space however none that rendered the RSA system insecure. Another category of powerful and sensible public-key schemes was found by ElGamal in 1985.

One of the foremost important contributions provided by public-key cryptography is that the digital signature. In 1994 the U.S. Government adopted the Digital Signature normal; a mechanism supported the ElGamal public key theme. To explore for new efficient public-key schemes, enhancements to existing scientific discipline mechanisms and proofs of security continues at a speedy pace. Security product square measure being developed to handle the safety wants of associate degree data intensive society. The aim of this paper is to outline the key concepts involved in two algorithms namely Goldwasser-Micali (GM) encryption and most widely used RSA. Some of the metrics used for comparison are encryption time, decryption time and size of cipher text with varying plain text sizes which are the key considerations for choosing an encryption algorithm. The comparison of encryption and decryption time with varying plain text sizes for both the algorithms using math lab code and preliminary observations are depicted in this paper.

2. Review of literature

The following literatures discuss various aspects of RSA and Probabilistic algorithms with reference to their speed and cipher text size individually. Glance of the core content of each papers are discussed below.

Shafi Goldwasser et. al provides the specified number-theoretic ideas and also the notion of linguistics security is conferred in an off-the-cuff approach [1] to the probabilistic encryption schemes. Digital watermarking systems are accustomed demonstrate possession of and imbed information in transmission signals. Based on the randlet remodel, Manuel Blum et. al. proves basis of strong encryption scheme[2]. Digital signature theme supported the process issue of number factorization. The theme possesses the novel property of being strong against associate adaptive chosen-message attack [3].

Adam.L.Young et. al in his research describes a brand new trapdoor-knapsack public-key cryptosystem[4]. The encoding equation is predicated on the final standard backpack equation, but, in contrast to the Merkle-Hellman theme, the backpack parts don't ought to have an excellent increasing structure. The Rivest, Shamir, and Adleman (RSA) public-key encoding rule are often broken if the number used because the modulus are often factored. It may but be potential to interrupt this technique while not resolution and this is explained by Williams et. al. [5]

RSA cryptography and its modification for efficiency and reliability over the networks like WiFi are explained by Venkatsatyavivek et. al . It gives the solution for some of the security vulnerability. The solution is based on random number generation process and several encryption and decryption algorithm. Sonam Mahajan et. al describes the main fundamental problem of RSA algorithm such as speed and use of poor or small prime numbers that has led to significant security holes despite the RSA algorithm's mathematical soundness can be alleviated by this algorithm[7].

SilviaHeubach et. al describes another method of probabilistic algorithm for obtaining an approximate empirical distribution function for the latency times using the iterative rollback method [8]. Behavioral approaches to probabilistic algorithms were discussed by Gabe Merrill et. al. in his research [9]. It describes a methodology for programming robots knows as probabilistic robotics. Minimizing vulnerability over the network by utilization of data transformation or encryption/decryption techniques among senders and receivers to achieve secure communication is discussed by L. Ham et. al. [10].

3.0 Brief Overview of RSA and GM algorithms

3.1 RSA encryption

The RSA cryptosystem, named once its inventors R. Rivest, A.Shamir, and L.Adleman, is that the most generally used public-key cryptosystem. It should wont to offer secrecy and digital signatures and its security relies on the trait of the whole number resolution.

The rule was proprietary by university in 1983 within the United States of America as U.S. Patent 4405829. It expired twenty one Gregorian calendar month 2000. Since the rule has been printed before application, rules in a lot of the remainder of the globe precluded patents elsewhere. Had Cocks' work been publically acknowledged, a patent within the North American nation wouldn't are attainable either.

3.1.1 Key Generation in RSA encryption

Suppose a user A wishes to allow B to send her a private message over an insecure transmission medium. She takes the following steps to generate a public key and a private key

Step:

1. Choose two large prime numbers $p \neq q$ randomly and independently of each other.
2. Compute $= p * q$.
3. Compute $\theta=(p-1)(q-1)$;
4. Choose an integer $1<e<\theta$ which is co-prime to θ.
5. Compute d such that $de = 1 \pmod{\theta}$.

Numbers can be probabilistically tested for primality. A popular choice for the public exponents is $2^{16} + 1 = 65537$. Some applications choose smaller values such as 3, 5, or 35 instead.

This is done to make encryption and signature verification faster on small devices like smart cards but small public exponents may lead to greater security risks. Steps 4 and 5 can be performed with the extended Euclidean algorithm.

3.2 The Goldwasser-Micali Encryption Scheme

It is the 1st probabilistic public-key encryption1, that means that the same message encrypted different times produce different cipher texts. The cryptosystem works at a bit level.

The security of the algorithm is based on the difficult problem of making a decision about quadratic residuosity of x modulo n = p*q without knowing p and q. We present the three algorithms K, E and D of the Goldwasser-Micali encryption scheme as given below.

3.2.1 Algorithm 1 [Key Generation K]

1. Select two large random primes p and q, p≠q.
2. Set n←pq.
3. Select a pseudosquare y € Zn (i.e. y is quadratic non-residue and (y/n) = 1).
4. The public key is (n, y), the private key is (p, q).

3.2.2 Algorithm 2 [Encryption E]

Let message m be a binary string m = m1,m2 . . .ml let (n, y) be the public key.

1. For i = 1. . .l do:

(a) Select x€ Z_n at random.

(b) If $m_i = 0$, set ci← x2 mod n; otherwise set $c_i \leftarrow yx^2$ mod n.

2. The ciphertext is c = (c_1, c_2, . . . , c_l)

3.2.3 Algorithm 3 [Decryption D].

Let c = (c_1, c_2, . . . , cl) be a cipher text and (p, q) the private key.

1. For i = 1. . .l do:

(a) Compute ei = (cip) e_i=(c_i/p)using Proposition 1.

(b) If e_i= 1, set mi←0; otherwise set mi←1.

2. The decrypted message is m = (m_1,m_2, . . . ,m_l).

3.2.4 Properties of Goldwasser-Micali Encryption

- Adds a significant amount of redundancy to the initial message. Each bit is sent as an element ci of Z_ n. Typically, the expansion is of 1 to 1024 bits.
- Each message bit is encrypted in a fully independent way. More than a block cipher, it is a stream cipher.
- Used in certain protocols such as: Phone coin ipping", Mental poker playing" and Minimum knowledge proofs".
- Much faster to encrypt and decrypt than the respective block-based public- key encryption methods such as the RSA, etc.
- There are other versions (Blum-Goldwaser 1984) that reduce the added redundancy by using numbers n that have special characteristics.

4.0 Performance evaluation of algorithms

The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in converting and sending the data in the network. The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. Performance evaluation has been studied using in MATLAB 8.6, 2015. An algorithm was developed in Math lab for implementation and evaluation of these algorithms. The screen shot of the same is given in Fig. 1.

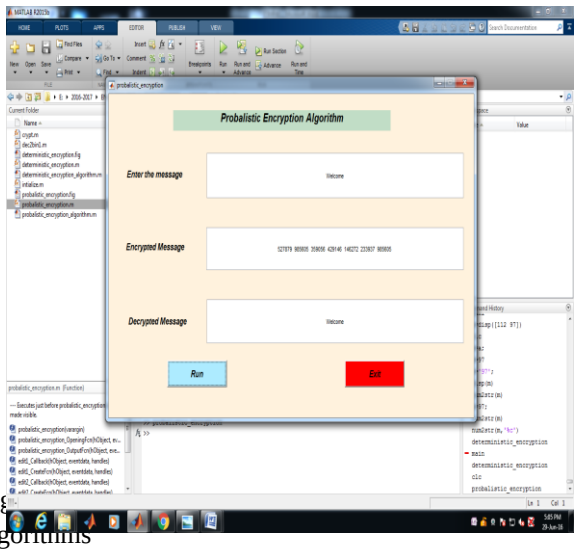

Fig. of algorithms

Two different message sizes up to 30 bytes of data are inputted to these algorithms and corresponding encryption & decryption time were measured. Random bits of data

are generated data for each byte of data and the experiment is repeated several times and execution times are averaged to get execution time. The Encryption time and decryption time taken by RSA (deterministic algorithm) and Probabilistic algorithm is shown in Fig 2. and Fig 3. respectively. The graph shows that the encryption and decryption time taken by probabilistic algorithm is always less than the RSA algorithms for various plain text sizes. Hence, it is evident that the speed of the probabilistic algorithms is more compared to the RSA algorithms.

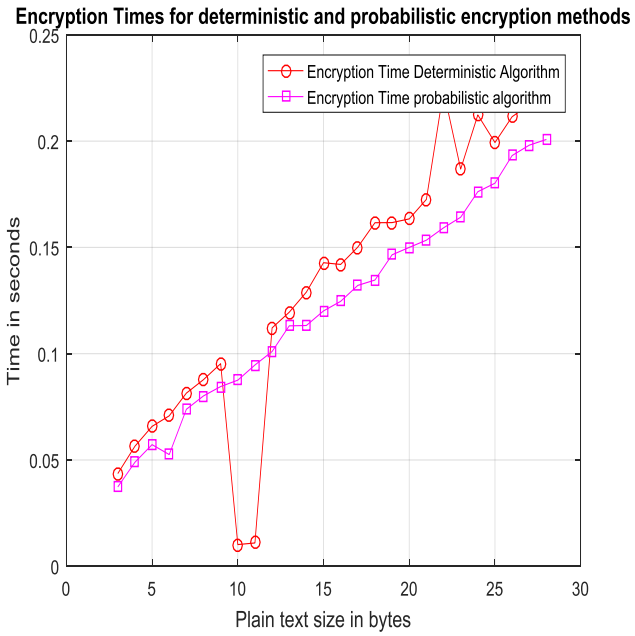

Fig 2 Encryption time taken by cryptographic algorithms

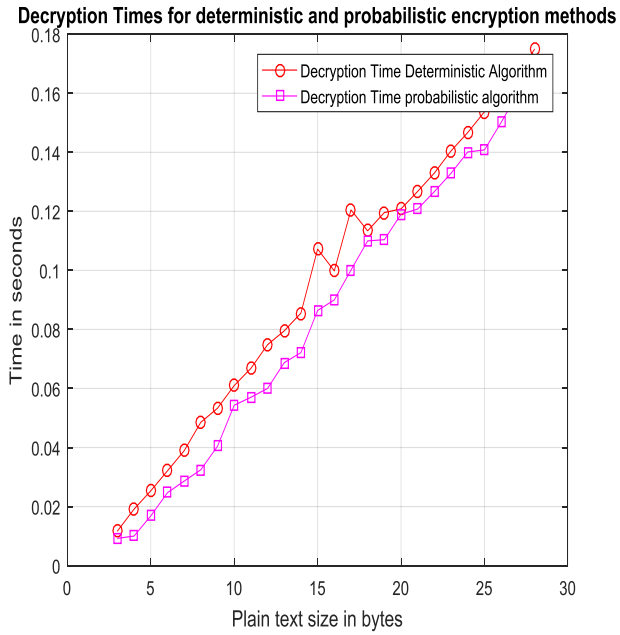

Fig 3. Decryption time taken by cryptographic algorithms

Message bytes	Method	Encryption Time	Decryption Time
3bytes	Deterministic encryption	0.0435	0.0116
	Probabilistic Encryption	0.0243	0.0092

Encryption and decryption time for various plain text are tabulated in Table 1, Table 2 and Table 3. It is evident from the data that the probabilistic algorithm takes less time both for encryption and decryption for message sizes from 3 bytes up to 260 bytes. Hence, the algorithm can be very well used for encryption and decryption of data in the network with suitable modification.

Table 1.Encryption and Decryption Time for 3 Byte Input

Message bytes	Method	Encryption Time	Decryption Time
28 bytes	Deterministic encryption	0.2214	0.1749
	Probabilistic Encryption	0.2001	0.1087

Table 2. Encryption and Decryption Time for 28 Byte Input

Message bytes	Method	Encryption Time	Decryption Time
260 bytes	Deterministic encryption	1.8584	1.7644
	Probabilistic Encryption	0.6832	0.5684

Table 3. Encryption and Decryption Time for 260 Byte Input

Goldwasser and Micali develop a little coding perform supported the quantity hypothetical drawback of quadratic residuosity. The tactic has several helpful properties. However there is one major drawback in probabilistic algorithm, that for a given security parameter N, the probabilistic coding of every bit is N bits long, needs N random bits, and uses many operation on N bit integers. A major disadvantage of the Goldwasser-Micali theme is that the message enlargement by an element of n bits. Some message enlargement is inescapable during a probabilistic coding theme as a result of their area unit several cipher texts equivalent to every plaintext. The jolly penolah a dense methodology of probabilistic coding that, in contrast to the tactic Goldwasser and Micali, is capable of encrypting over one bit at time. For any given k and security parameter N, this new methodology permits the coding of k bits of data into AN N + k bit cipher text victimization N + k random bits and operations on N + k bit integers. Thus, for any desired security parameter N, the magnitude relation of plaintext size to cipher text size (as well on random bits needed or to the scale of the integers computed upon) is created indiscriminately near

one. During this implementation the settled and probabilistic coding Schemes time consumption area unit is carried out.

5.0 Conclusion

Performance of Goldwasser -Micali algorithm and RSA encryption algorithm were compared in this study. The encryption and decryption algorithm were implemented using MATLAB with different plain text sizes and encryption and decryption timing were calculated. The results shows that Goldwasser-Micali algorithm takes less time in decrypting and encrypting than RSA algorithm. However the Goldwasser-Micali scheme has a disadvantage of message enlargement by an element of n bits. Hence, with suitable modifications in the probabilistic algorithm, there is a definite potential that it can be used as a high speed algorithms for cryptography.

References

[1] ShafiGoldwasser and Silvio Micali, "Probabilistic Encryption" Laboratory of computer science, Massachusetts institute of technology, Cambridge, Vol.28, No.2, 1984.

[2] Manuel Blum and Silvio Micali, "How To Generate Cryptographically Strong Sequences Of Pseudo Random Bits" Department of Elecrical Engineering and Computer Sciences, University of California, Berkeley, IEEE ,1982

[3] ShafiGoldwasser , Ronald L. Rivest and Silvio Micali, "a digital signature scheme secure against adaptive chosenmessage attacks,", Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Vol. 17, No. 2, 1988.

[4] Dr.Adam.L.Young and Dr.Moti.L.Young, "Malicious Cryptography exposing cryptovirology," Wiley Publishing, Inc., Indianapolis, Indiana, 2004

[5] Williams." A modification of the RSA public-key encryption procedure" IEEE Transactions on Information Theory , Volume:26 , Issue: 6, 1980.

[6] T.Venkatsatyavivek," Modified RSA algorithm for (wi-fi) security protocol"(9IJCSIT)International Journal of Computer science and Information Technologies, Vol 6(3), 2015.

[7] Sonam Mahajan and Maninder Singh "Analysis of RSA algorithm using GPU programming. Department of Computer Science Engineering, Thapar University, Patiala, IndiaIndiaInternational Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, 2014

[8] SilviaHeubach, RajS.Pamula"Implementing an approximate probabilistic algorithm for error recovery in concurrent processing system" Dept.of Mathematics and computer science,California state university,LosAngeles. (http://web.calstatela.edu/faculty/sheubac/papers/AoMpaper.PDF)

[9] R. Gabe Merrill and Mark Andraschko "Probabilstic algorithm is Robotics."Analytical Mechanics Associates Inc, Hampton, Virginia. (http://robots.stanford.edu/papers/thrun.probrob.pdf)

[10] L. Harn and D. Huang., "A protocol for establishing secure communication channels in a large network" IEEE Transactions on Knowledge and Data Engineering, Volume:6 , Issue: 1, 1994.

Author Profile

Ms. N. Priya completed Bca and MSc Degrees in Computer science from Vidhyasar Women's College, Madras university, India in 2011 and 2013, respectively. Presently, she is pursuing her Mphil degree from SCSVMV University, Kancheepuram, Tamilnadu, India. Her areas of interests are Network security, Software engineering and Semantic web applications.