Amit Rajendra Garge *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 10, October- 2015, pg. 59-65 **ISSN: 2321-8363**

RSA and ELGamal Cryptosystem: An Overview

Amit Rajendra Garge[1], Chetna Subhash Ghebad[2], Sonal Sarnaik[3], Surbhi Thorat[4]

[1] Student, TYMCA (A), MIT (E) College, Aurangabad (M.S.). amit.garge19@gmail.com
[2] Student, TYMCA (A), MIT (E) College, Aurangabad (M.S.). chetna.ghebad123@gmail.com
[3]Asst. Prof.MCA Dept. MIT (E) College, Aurangabad (M.S.). sonalsarnaik141@gmail.com
[4]Asst. Prof.MCA Dept., MIT (E) College, Aurangabad (M.S.). thorat.surbhi@gmail.com

Abstract

Cryptography is an art of information security, whose fundamental objective is the security of the message which is being transferred through an insecure medium between two parties i.e. sender and the receiver. There are two Cryptosystem: private and public key cryptosystem. This paper is about the overview of the two public key cryptography systems RSA and ElGamal Cryptosystem. RSA uses the base of Integer Factorization while ELGamal Cryptosystem uses the base of Discrete Logarithm Problem.

Keywords: Cryptography, Public Key Cryptography, Modular Arithmetic, Integer Factorization, Discrete Logarithmic Problem, RSA, ElGamal Cryptosystem.

1. Introduction

Cryptography is an art of information security, whose fundamental objective is the security of the message which is being transferred through an insecure medium between two parties i.e. sender and the receiver. There are two types of cryptography algorithms; namely private or symmetric key algorithm and public or asymmetric key algorithm. In private or symmetric key algorithm the key of encryption and decryption is same. While in public or asymmetric key algorithm the key of encryption is the public key (which is mutually discussed between sender and the receiver) and the decryption key. Symmetric key cryptography is based on the sender and receiver of messages knowing and using the same secret key. The sender uses the secret key to encrypt the message and the receiver uses the same secret key to decrypt it [1] [5] [6][8][9].

Public Key and Private Keys: The Public and Private Key pair comprise of two uniquely related cryptographic keys basically long random numbers. The Public Key is what its name suggests – Public, It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential to its respective owner. Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa [5][8][9]. Public key cryptography is used where each user has a pair of keys, one called the public key and the other private key. Each user's public key is published while the private key is kept secret and thereby the need for the sender and the receiver to share secret information (key) is eliminated. The only requirement is that public keys are associated with the users in a trusted (authenticated) manner using a public key infrastructure (PKI). The public key cryptosystems are the most popular, due to both confidentiality and authentication facilities. PKC depends upon the existence of one way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute[8][9].

Public key Cryptosystem:

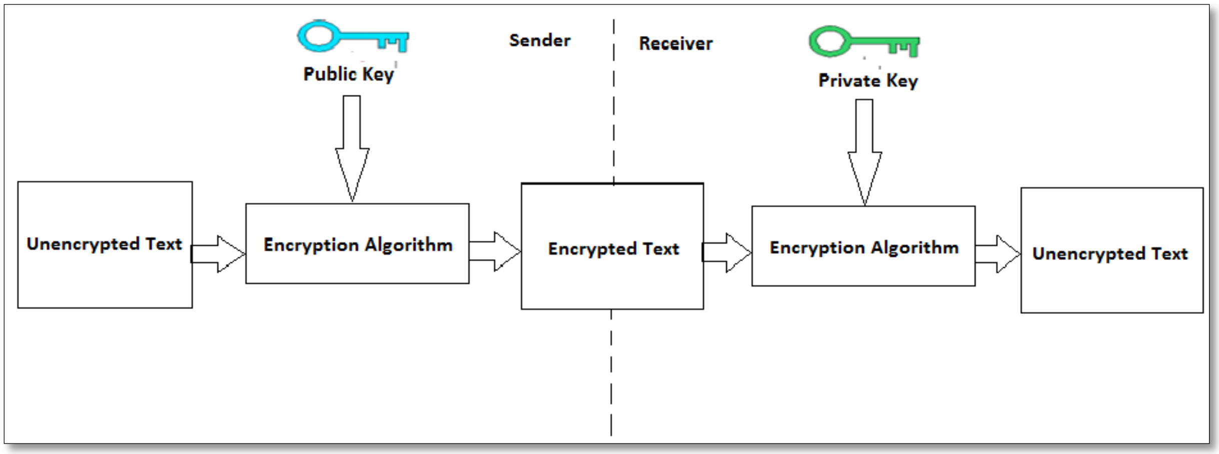

Figure 1: Public key Cryptosystem

2. Mathematical foundation

2.1 Modular Arithmetic:

Mod-arithmetic is the central mathematical concept in cryptography. Any cipher from Caesar Cipher to RSA Cipher uses it.“Modulus” (abbreviated as "mod") is the Latin word for “remainder, residue” or more in “what is left after parts of the whole are taken”. Thus, "modular" or "mod arithmetic" is really "remainder arithmetic". More precise: We are looking for the integer that occurs as a remainder (or the "left-over") when one integers is divided by another integer [5][8][9].Modular Arithmetic is also called Clock Arithmetic.

Example 1:

132 mod 13=2

132 mod 13=2	145 mod 13=2
133 mod 13=3	146 mod 13=3
134 mod 13=4	147 mod 13=4
135 mod 13=5	148 mod 13=5
136 mod 13=6	149 mod 13=6
137 mod 13=7	150 mod 13=7
138 mod 13=8	151 mod 13=8
139 mod 13=9	152 mod 13=9
140 mod 13=10	153 mod 13=10
141 mod 13=11	154 mod 13=11
142 mod 13=12	155 mod 13=12
143 mod 13=0	156 mod 13=0
144 mod 13=1	157 mod 13=1

This cycle repeats from 0 to 12 with mod operation of 13

2.2 Integer Factorization:

In number theory, integer factorization is the decomposition of a composite number into a product of smaller integers. If these integers are further restricted to prime numbers, the process is called prime factorization. When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known; an effort by several researchers concluded in 2009, factoring a 232-digit number (RSA-768), utilizing hundreds of machines over a span of two years. [1][7] [8][9]

Given two primes, say p = 863 and q = 877, it is an easy process to multiply them by hand to get the product n = 756851. However, it is not nearly so easy to determine by hand the factors p and q from only knowledge of the product 756851. In a similar fashion, if p and q are large, say 1,000 digits each, then a computer can readily find the 2,000 digit product (since multiplying two k-digit numbers requires at most tex2html_wrap_inline854 operations), but even the fastest of today's computers cannot generally determine the factors from only the product. This leads us to consider two central problems in the history of mathematics, namely the problems of (a) determining whether a given integer is a prime, and (b) determining the factorization into primes of a given integer[8][9].

2.3 Discrete Logarithm Problem:

If a is an arbitrary integer relatively prime to n and g is a primitive root of n, then there exists among the numbers 0, 1, 2, ..., phi(n)-1, where phi(n) is the totient function, exactly one number mu such that ,**a=g^mu (mod n)**.

The number mu is then called the discrete logarithm of a with respect to the base g modulo n and is denoted **mu=ind_ga (mod n).**

The term "discrete logarithm" is most commonly used in cryptography, although the term "generalized multiplicative order" is sometimes used as well , In number theory, the term "index" is generally used instead .

For example, the number 7 is a positive primitive root of n=41 (in fact, the set of primitive roots of 41 is given by 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35), and since 15=7^3 (mod 41), the number 15 has multiplicative order 3 with respect to base 7 (modulo 41).

The generalized multiplicative order is implemented in the Wolfram Language as Multiplicative Order [g, n, {a1}], or more generally as Multiplicative Order[g, n, {a1, a2, ...}].Discrete logarithms were mentioned by Charlie the math genius in the Season 2 episode "In Plain Sight" of the television crime drama NUMB3RS. [1][8][9]

3. RSA ALGORITHM

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. Many protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. It is also used in software programs -- browsers are an obvious example, which need to establish a secure connection over an insecure network like the Internet or validate a digital signature. RSA signature verification is one of the most commonly performed operations in IT.RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total -- factoring -- is considered infeasible due to the time it would take even using today’s super computers[5][8][9][10][11][12][14][15].

Table 1: Stepwise representation of RSA algorithm

Alice	**Publically Declared Values**	**Bob**
Step 1: Alice will choose Two large prime number p and q Find n= p*q. Calculate: ɸ(n)=(p-1) *(q-1)		
Step 2: Choose e such that it satisfies Following condition. i. GCD(e,ɸ(n))=1 ii. Max(p, q) iii. e must be prime no		
Step 3: Find d such that it satisfies:- i. e. d ≡ 1 mod ɸ(n) ii. d>log2(n) iii. GCD(d,ɸ(n))=1	n and e	M is message to send
Step 4: $C=M^{e}$ mod n	Cipher text is send to Alice	
Step 5: Original message is derived by ,$M=C^{d}$ mod n		

Where e is the encryption key which is publically declared, d is decryption key which is private, M is the Original Message and C is the Cipher text generated.

Example:

Step 1: p=103,q=113
n= p*q
n=103*113
n=11639
ɸ(n)=(p-1)*(q-1)
=(103-1) *(113-1)
=11424

Step 2: If we choose e=5563 then it should satisfy.
i. GCD(e, ɸ(n))=1
GCD(5563,11424)=1 ---Condition satisfy
ii. Max(p,q)
Max(103,113)=113
so, e>113 i.e e=5563 ---Condition satisfy
iii. 5563 is a prime number ---Condition satisfy

Step 3: Find d such that it satisfies:-

i. e. d ≡ 1 mod ɸ(n)
ii. Will try possibility for d from 1 till it satisfies the equation.

Table 2: Iterations of e. d ≡ 1 mod ɸ(n)

e	e. d mod ɸ(n)≡ 1 mod ɸ(n)	Status
1	1*5563 mod 11424 =5563	Cannot use
2	4*5563 mod 11424 =10828	Cannot use
3	2*5563 mod 11424 =11126	Cannot use
4	5*5563 mod 11424 =4967	Cannot use

5	3*5563 mod 11424 =5265	Cannot use
6	115*5563 mod 11424=1	Can be used

ii. e>log2(n)
115>13.50667949[condition satisfy...]

iii. Gcd(e, φ(n))=1
GCD(115,11639)=1
So, e=5563 and n=11639 [condition satisfy...]

4. ELGamal Cryptosystem:

El-Gamal encryption/decryption is based on the difficulty of the discrete algorithm problem where it is straight forward to raise numbers of large powers but it is much harder to do the inverse computation of the discrete logarithm. The ElGamal algorithm depends on certain parameters which are affecting the performance, speed and security of the algorithm. The importance of these parameters and role it takes in the security and the complexity of the system and the analyzed, particularly the effect of changing the length of modulo number and the private key number are investigated. ElGamal encryption is one of many encryption schemes which utilize randomization in the encryption process. [3][8][9]

Table3: ELGamal Public Key Encryption Algorithm:

Alice	**Mutually Discussed (g, p)**	**Bob**
Step 1: Chooses a secret key ‘a’		**Step 1:** Chooses a secret key ‘b’
Step 2: A= g^a mod p	**A** →	**Step2:** B=g^b mod p
		Step 3: Key_{enc}= A^b mod p
		Step 4: C=Key_{enc}*Message
Step 5: Key_{dec}= B^a mod p	**B, C** ←	
Step 6: Key_{dec}^{-1}= 1 mod p		
Step 5: Message = Key_{dec}^{-1} * C		

Table4: ELGamal Public Key Encryption Algorithm Example

Alice	**Mutually Discussed (g, p)**	**Bob**
Step 1: a=4	g=2, p=13	**Step 1:** b=3, Message=7
Step 2: A= g^a mod =2^4 mod 13 **A=13**	**A** →	**Step 2**: B=g^b mod p =2^3 mod p **B=8**
		Step 3: Key_{enc}= A^b mod p = 3^3 mod 13 **Key_{enc}=1**
		Step 4: C= Message * Key_{enc} =7 * 1 **C=7**
Step 5: Key_{dec}= B^a mod p = 8^4 mod p **Key_{dec}=1**	**B, C** ←	
Step 6: Key_{dec}^{-1}= 1 mod p **Key_{dec}^{-1}=1**		
Step 7: Message = Key_{dec}^{-1} * C = 1 * 7 **Message= 7**		

5. Conclusions:

This paper discusses about Cryptography, an art of Information Security, with its two types: private key cryptography and public key cryptography. In the public Key Cryptosystem there are two keys: public and private key. Sender uses public key to encrypt the message before sending the message to the receiver. And Receiver uses its private key to decrypt the message. This paper also includes the overview of two public key cryptosystem: RSA and ELGamal Cryptosystem. Modular Arithmetic is the base of Modern Cryptography. RSA is based on Integer Factorization and ELGamal Cryptosystem is based on Difficulty of Discrete Logarithmic Problem.

References:

[1] *"Cryptography and Encryption"* KOSTAS ZOTOS, ANDREAS LITKE Dept. of Applied Informatics, University of Macedonia 54006 Thessaloniki, GREECE {zotos, litke}@uom.gr.

[2] *"NATIONAL INSTITUTE OF SCIENCE TECHNOLOGY"*, ODISHA, INDIA Kuna Siva Sankar Student B.tech (CSE) .3rd Year Institute: RGU IIIT, Nuzvid, AP. Email: sankar.kuna@gmail.com

[3] *"Elgamal's Algorithm in Cryptography"* Rashmi Singh, Shiv Kumar (M.Tech.) Mewar University NH - 79 Gangrar,(Rajasthan) - 312901 Ph. 9694430530 Email_id: rashmikamal011@gmail.com

[4] "*Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm*".,© 2012, *IJARCSSE* All Rights Reserved Volume 2, Issue 8August 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com

[5] "*An overview and cryptographic challenges of RSA*" B Hawana, IJERMT, 2013.

[6] " *A survey of fast exponentiation methods* ", Daniel M. Gordan, , 1997.

[7] "*New Directions in Cryptography*", Whitfield Diffie and Martin E. Hellman, , IEEE Transactions on Information Theory, 22(6):644-654, 1976.

[8] "*An Algorithm For Factoring Integers*", Yingpu Deng and Yanbin Pan,.

[9] "*Handbook of Applied Cryptography*", Menezes, Alfred J; van Oorschot, Paul C.; Vanstone, Scott A. (2001),.

[10] "*Cryptography: Theory and Practice (3rd ed.)*", Stinson, Douglas Robert (2006), , London: CRC Press.

[11] "*CRYPTANALYTIC ATTACKS ON RIVEST, SHAMIR, AND ADLEMAN (RSA) CRYPTOSYSTEM: ISSUES AND CHALLENGES*".Adamu Abubakar, Shehu Jabaka, Bello Idrith Tijjani,

[12] "*A survey on performance Analysis of DES, AES and RSA algorithm along with LSB substitution technique*"B. Padmavati, S. Ranjitha Kumari, 2013.

[13] "*Traditional Cryptography: A Mathematical overview*". Sonal Sarnaik, Nilesh Jaibhai, Rutuja Sontakke,

[14] "*CRYPTANALYSIS OF SHORT RSA SECRET EXPONENTS*" Michael J. Wiener, 1989 August 3.

[15] "*PROOF CHECKING THE RSA PUBLIC KEY ENCRYPTION ALGORITHM*" Robert S. Boyer and J Strother Moore,. September 1982.

A Brief Author Biography

Amit Rajendra Garge – Student of Third year of Master of Computer Application (Under Engineering and Technology) of Marathwada Institute of Technology(E), Aurangabad(M.S.). Completed B. Sc. (C.S.), Research interests are Cryptography, Computer Networks, and Network Layer.

Chetna Subhash Ghebad – Student of Third year of Master of Computer Application (Under Engineering and Technology) of Marathwada Institute of Technology(E), Aurangabad(M.S.). Completed B. Sc. (C.S.), Research interests are Cryptography.

Sonal Sarnaik – Asst. Prof., MCA Dept. of Marathwada Institute of Technology(E), Aurangabad(M.S.). Completed B. E..(CSE), Research interests are Cryptography, Mobile Computing and Image Processing.

Surbhi Thorat – Asst. Prof., MCA Dept. of Marathwada Institute of Technology(E), Aurangabad(M.S.). Completed MCA, Research interests are Data Warehousing, Cryptography.