Journal of Physics: Conference Series

A Crypto Compression System Using ElGamal Public Key Encryption Algorithm and Even-Rodeh Codes

To cite this article: M A Budiman *et al* 2020 *J. Phys.: Conf. Ser.* **1566** 012071

A Crypto Compression System Using ElGamal Public Key Encryption Algorithm and Even-Rodeh Codes

M A Budiman[1], E M Zamzami[2], C L Ginting[3]
[1]Department of Computer Science, Faculty of Computer Science and Information Technology Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

*Email: mandrib@usu.ac.id, elvi_zamzami@usu.ac.id, and cindylaurentginting@gmail.com

Abstract. Confidentiality and size of data are some significant aspects in data exchange. Public key encryption algorithms, such as El-Gamal is known as to preserve confidentiality. On the other hand, public key encryption algorithms tend to increase the size of the encrypted data, making it difficult to transmit to the other party. This research will combine the ElGamal public key encryption algorithm with Even-Rodeh codes. ElGamal is used to secure data and Even-Rodeh codes are used to compress data. The parameters is being tested are the compression ratio and space savings. In this research, we will do an experiment that includes some data texts from Artificial Corpus. The results show that the crypto compression system can reduce the size of the transmitted data and the transmitted data could be revert back to the original data while still maintains its confidentiality.

1. Introduction

Cryptography is the science of using mathematics to convert the information content or message into secure form, making it less immune to attack [1]. Converting the original message (plaintext) into a secure message could be thought of as combination of art and science [2]. There are two cryptographic types: Symmetric Key and Asymmetric Key. ElGamal is an asymmetric key encryption algorithm based on Diffie-Hellman’s key exchange which Taher Elgamal described in 1985 [3]. The security of ElGamal relies on the difficulty of computing discrete logarithms in a large primary factor [3]. ElGamal encryption for each plaintext gives a distinct cipher text [4]. The encryption process is carried out on each bit to allow the enlargement of the data size [4]. Thus, the cipher text length is longer than the plaintext. Hence, data compression is required.

Data compression is a method for reducing the size of data to store it much more compactly and to reduce its transfer time [5]. It has been commonly used in many fields of data processing, such as text files, images, videos, etc [6]. Data compression is separated into two different types: lossless and lossy compression. Even-Rodeh Code is a lossless compression that allows the compressed data to be reconstructed back to the original data [5]. This is a Variable Length Code (VLC) that has different bits used by the code to express each symbol [5]. Even-Rodeh Code was developed by Shimon Even and Michael Rodeh.

In this research, an experiment will be conducted that combines ElGamal to encrypt the data text with Even-Rodeh Code to compress. The text data is obtained from the corpora files: The Artificial Corpus (http://www.corpus.canterbury.ac.nz/descriptions/).

2. Method

In this section, we are explains El-Gamal computation and how Even-Rodeh Code works. First, data text with the El-Gamal algorithm will be encrypted and testing prime numbers using the Agrawal-Biswas algorithm. Then the encryption outcomes will be compressed using Even-Rodeh Code algorithm, and finally, the decryption method will be completed once the text has been decompressed. There are five processes namely: key generation, encryption, decryption, compression, and decompression.

2.1. El-Gamal Algorithm

2.1.1. Key Generation

This process generates public key and private key for both encryption and decryption. The sender only knows the public key and the recipient knows the private key as well as the public key.

1. Generate a large prime number p with Agrawal-Biswas primality test. The step is stated as follows:
   a. Generate a large random number p to be tested, with $p >$ total table characters.
   b. Generate random number z with $3 < z < p - 2$.
   c. If $(1 + z)^p \bmod p = (1 + z^p \bmod p) \bmod p$, then p is prime.
   d. If not, return to the step 1.
2. Generate α as a primitive root of p.
3. Generate an integer a with $2 < a < p - 2$.
4. Compute $x = \alpha^a \bmod p$.
5. Get (p, α, x) as the public key and (a) as the private key.
6. Generate random number b with $b < p - 2$.
7. Compute $y = \alpha^b (mod\ p)$.
8. Compute $z = (\alpha^b)^{(p-1-a)}\ mod\ p$
   Because $y = \alpha^b (mod\ p)$, $z = y^{(p-1-a)}\ mod\ p$.

2.1.2. Encryption

In this process, the data text will be encrypted with the key that has been raised.

1. Input the message.
2. Encrypt the data text with calculation $c = m * [x^b\ mod\ p]\ mod\ p$.

2.1.3. Decryption

This process the encrypted data text (cipher text) will be returned to the original text. The steps of encryption process are as follows:

1. Get the message and the private key (z).
2. Decrypt the message with calculation $m = c * z \bmod p$.

2.2. Even-Rodeh Code Algorithm

The steps to generate an Even-Rodeh code are stated as follows:

1. If $n < 4$ then code word is the binary representation of n and the length of code is (3 – length(code)) times ‘0’ prepended to the code.
2. If $n >= 4$ and $n < 8$ then prepend ‘0’ to the binary representation of n.
3. If $n >= 8$ then code word is the binary representation of n, prepend the representation of length code in binary to the code and prepended again to ‘0’

Table 1. Several Even Rodeh Codes and Its Different Lengths

	Even-Rodeh Code	Values	ER Length
0	000	0-3	3
1	001		
2	010		
3	011		
4	100 0	4-7	4
7	111 0		
8	100 1000 0	8-15	8
15	100 1111 0		
16	101 10000 0	16-31	9
32	110 100000 0	32-63	10
100	111 1100100 0	64-127	11
128	100 1000 10000000 0	128-255	16
256	100 1001 100000000 0	256-512	17

3. Results and Discussion

Consider to the case, assume that Cici (sender) would like to send a message to Kiki (recipient) that is a ‘C’ letter. El-Gamal algorithm will be utilized by Cici and Kiki. Kiki generates a random asymmetric key (public key and private key). Then, Kiki will send his public key to Cici, the public key is used to encrypt her message and the encrypted message will be sent to Kiki. Then, Kiki will decrypt the encrypted message with his private key.

A. Key Generation (Kiki)

1. Generates Generate a large prime number p = 919with Agrawal-Biswas primality test. The step is stated as follows:
   a. Generate random number Z = 460with 3 <Z < p – 2.
   b. Calculate $(1 + Z)^p$ mod p = (1 + Z^p mod p) mod p
   $$(1+Z)^P \text{ mod } p = (1 + Z^P \text{mod p})$$
   $$(1+460)^{919} \text{ mod } 919 = (1 + 460^{919} \text{mod } 919)$$
   $$461 = 461$$
   Because the calculation result is equivalent, 919 is a prime.
2. Generate α = 7 as a primitive root of p.
   - Calculate $q = \frac{p-1}{2} = \frac{919-1}{2} = 459$
   - Calculate $\alpha^2 \; mod \; p = \; \alpha^q \; mod \; p$
   $$\alpha^2 \; mod \; p = \; \alpha^q \; mod \; p$$
   $$7^2 \; mod \; 919 = \; 7^{459} \; mod \; 919$$
   $$49 = 918$$
   Because$7^2 \; mod \; 919 \neq 1$ and $7^{459} \; mod \; 919 \neq 1$, α is a primitive root.
3. Generate an integer a = 690 with 2 <a<p – *2.*
4. Compute x = α^a mod p.
   $$x = \alpha^a \; mod \; p$$
   $$= \; 7^{690} \; mod \; 919$$
   $$= 895$$
5. Get (p, α, x)= (919, 7, 895) as the public key and (a) = (690) as the private.
6. Generate random number b = 173 with b<p – 2.
7. Compute $y = \alpha^b \; (mod \; p)$.
   $$y = \alpha^b \; mod \; p$$
   $$= 7^{173} \; mod \; 919$$
   $$= 294$$

8. Compute $z = (\alpha^b)^{(p-1-a)}$ *mod p.*
Because $y = \alpha^b$ *(mod p)*, $z = y^{(p-1-a)}$ *mod p.*

$$\begin{aligned} z &= (y)^{(p-1-a)}\ mod\ p \\ &= (294)^{(919-1-690)}\ mod\ 919 \\ &= (294)^{(228)}\ mod\ 919 \\ &= 460 \end{aligned}$$

B. Encryption (Cici)

1. Input the message 'C' = 67 (ASCII Code)
2. Encrypt the text with calculation $c = m * [x^b\ mod\ p]\ mod\ p$.

$$\begin{aligned} c &= m \times [x^b\ mod\ p] mod\ p \\ &= 67 \times [895^{173}\ mod\ 919] mod\ 919 \\ &= 67 \times 2\ mod\ 919 \\ &= 134 \end{aligned}$$

C. Decryption (Kiki)

1. Get the message '134'
2. Decrypt $m = c * z$ mod p

$$\begin{aligned} m &= c \times z\ mod\ p \\ &= 134 \times 460\ mod\ 919 \\ &= 67\ ('C') \end{aligned}$$

In this research, the result of the experiment is developed by using Artificial Corpus.

Table 2. The Experimental Result of the Artificial Corpus

No	Files (docx)	C_R[a]	S_S[b] (%)	Size (bits)		
				Plaintext	Cipher text Uncompressed	Cipher text Compressed
1.	a	2	50	8	32	16
2.	aaa	2.67	62	800.000	3.200.000	1.200.000
3.	alphabet	1.97	49	800.000	3.292.320	1.673.080
4.	random	1.94	49	800.000	3.298.096	1.698.088

[a]Compression Ratio
[b]Space Savings

Table 3. The Experimental Result of Office Documents

Files (docx)	C_R[a]	S_S[b](%)	Size (bits)		
			Plaintext	Cipher text Uncompressed	Cipher text Compressed
kpuimilkom	2.05	51	25.536	105.736	51.576
pdoimilkom	2.08	52	32.264	133.488	64.184
igtsimilkom	2.09	52	36.088	149.488	71.424
semnasimilkom	2.11	53	48.224	199.592	94.376

[a]Compression Ratio
[b]Space Savings

In table 1 and table 2, it can be seen that the average compression ratio is 2.11 and the average of space savings is 52,25% which means that Even-Rodeh Code can reduce the size of data enlargement from the El-Gamal encryption process.

Table 4. The Experimental results of Running Time system

No	Files (docx)	Encryption Compression	Decryption Decompression
1.	a	0.005	0.021
2.	aaa	0.631	1.13
3.	alphabet	0.778	1.22
4.	random	0.798	1.233
5.	kpuimilkom	0.03	0.05
6.	pdoimilkom	0.036	0.062
7.	igtsimilkom	0.041	0.069
8.	semnasimilkom	0.053	0.085
	Average	0.2965	0.48375

4. Conclusion

The conclusions of this research are that the El-Gamal algorithm can secure the information in the file. It has larger sizes after it has been encrypted and complicated to solve discrete logarithm, also the Even-Rodeh Code can compress the size of data text from the enlargement of El-Gamal encryption process, and the compressed data text can be decompressed into original text files without losing any information.

References

[1] Thakkar J 2015 An Encryption and Decryption More Secure El-Gamal Cryptosystem *Int. J. of Science Technology and Engineering* **1** 12

[2] Garg N and Partibha Y 2014 Comparison of asymmetric algorithms in cryptography J. of Computer Science and Mobile Computing **3** 4 1190-11196

[3] El-Gamal T 1985 A public key cryptosystem and a signature scheme based on discrete logarithms *IEEE trans. on information theory* **31** 4 469-472

[4] Singh R and Shiv K 2012 El-Gamal's algorithm in cryptography *Int. J. of Sci. & Eng. Res.* **3** 12 1-4

[5] Budiman M A and Rachmawaty D 2017 On Using Goldbach G0 Codes and Even-Rodeh Codes for Text Compression on Using Goldbach G0 Codes and Even-Rodeh Codes for Text Compression *IOP Conf. Series: Materials Sci. and Eng.* **180** 1.

[6] WalderJ, Kratky M, Baca R, Platos J and Snasel V 2012 Fast decoding algorithms for variable-lengths codes *Inf. Sci.* **183** 1 66-91.