INFORMATION DISSEMINATION ON THE INTERNET IN NIGERIA BASED ON SOME FUNCTIONS OF CRYPTOGRAPHY

Victor O. Waziri Ph.D.
Department of Cyber Security Science, School of Information and Communication Technology,
Federal University of Technology, Minna-Niger State, Nigeria
onomzavictor@gmail.com/ dronomzawaziri@yahoo.com

ABSTRACT

This paper presents a simple abstraction of some modern concepts of public--key exchange algorithms such as Pohlig-Helman Algorithms, Diffie-Hellman key Exchange, and ElGmal Cryptosystems. The models are very important in Security improvement especially in dispatching of Information on the Internet. All these models of Key management are explained with delineated conceptual simple mathematical frameworks. Besides, each Algorithm and cryptosystem is clarified with simple worked examples experimented in Matlab. By these simple worked numerical examples, Cryptography as a complicated Mathematical induction is brought down to a layman's frontier who has little mathematical background.

Keywords: Public-Key Exchange, Elgamal Cryptosystem, Diffie-Hellman Key, Matlab, Pohlig-Hellman Algorithms, Elgamal Signature.

1.0 INTRODUCTION

Information dissemination on the Internet network is generally a silky venture due to the unsecure nature of the network. Nigeria as a nation; as other nations, needs to have its Information on transition over the Internet network secured; this is more needing due to the current International terrorism and fees advance theft; amongst others. Globally, Information dissemination on the unsecure network can best be achieved through cryptography. Cryptography itself, nonetheless, is an intricate discipline that needs complete sound mathematical background. In the classical era, Cryptography was mainly an application of hiding information using one set of key-known as symmetric key. Today (ElGamal, 1985), cryptography has a wider spectrum of application apart from the confidentiality of information over the unsecure Internet network. Without attempting to provide a perfect definition of modern cryptography: *Cryptography is the scientific study of techniques for securing digital Information, transaction and distributed computations* (Abdallla *et al, 1985).*

Cryptographic methods are used to enforce access control in multi-user operating systems, and to prevent thieves from extracting trade secrets from stolen Laptops. In (Abdallla *et al*., 1985), software protection methods employ encryption, authentication, and other tools to prevent copying of most top state secretes.

The focus of this paper is based on modern Cryptography; otherwise, known as public-key encryption or asymmetric key encryption. In this paper, we focus on the algorithm use in key management (key exchange process). The basic key exchange is the Diffie-Hillman key exchange. The strength of this key exchange is assumed to be the discrete logarithm (DL). With an established key exchange of the Diffie-Hillman algorithm, we shall consider how to transmit information using the ElGamal cryptosystem.

The rest of this paper is as follows: Section 2 deals with the algorithm of the discrete logarithm algorithms. Section 3: desks with theoretical Diffie-Hillman system. Section 4: desks with the E/Gamal cryptography. In section 5: we fuse the three steps stirred into a comprehensive method to form our wholesome methodology; albeit in summary. Section 6: is our comprehensive research experimentation. This section experimental work shall be executed via a message encryption exercise.

2.0 RELATED WORKS

The entire body of Cryptography is an embodiment of much literature right from the documented period of Julius Caesar who propounded the Shift Cryptosystem (Menezes *et al*., 1985; Kenneth, 2006) to the modern Cryptography which is perceived to have begun with Diffie-Hellman public key exchange and dwelled upon by (ElGamal, 1985; Abdallla *et al*., 1985; Knobloch, 1993; Lim *et al.*, 1997; Lim and Lee, 1998 and Wenbo, 2003). Our concern in this research piece is based on modern cryptography which is generally known as public-key cryptosystem (Wenbo, 2003). As our focus is based on the modern public-key cryptosystems, and for want of space, we streamline our research into some of the current basic cryptosystems as given in the rest of this paper. Many interesting ancient literature of cryptography could be acquired in the documentation of classical cryptography (Kenneth, 2006) and others which abound abundantly in the literature of so many webpages.

3.0 DISCRETE LOGARITHM

Consider the expression $\log b^y = x$, then as we know from real numbers, this expression is equivalent to $b^x = y$. Furthermore, given integers b and n (Abdalla *et al*., 1985; Menezes *et al*., 1985), with $b < n$, the discrete logarithm of integer y to the base b is an integer x, such that:-

$$b^x \equiv y \bmod n \qquad 2.1$$

Discrete logarithm is also known as "index", and it is written as

$$x = ind_n^b y \qquad 2.2$$

Discrete logarithm is considered to be one-way function. In other words, the inverse computation of the discrete logarithm is much harder. The ElGamel system depends heavily on the difficulty of factorizing this algorithm.

4.0 DIFFIE-HELLMAN KEY EXCHANGE

One of the difficulties in the application of the symmetric key (or private key as is generally known) in classical cryptography is key management ElGamal (1985 and Abdalla *et al*., 1985). Key management is the process of distributing keys to the rightful owners without the man-in-middle intercepting them. In Diffie-Hellman algorithm, this dilemma of key distribution is solved. Diffie-Hellman key exchange forms the basis of the modern cryptosystem known as the public-key exchange. It is a seemingly simple an algorithm that goes in this order:

Consider two persons; Alice and Bob who are friendly and want to exchange secret pieces information via the insecure Internet communication system. Insecure because a third person who is an adversary called Eve can read the information on transition. It is the desire of Alice and Bob that the information on transmission in packages or datagrams through this insecure transmission system that Eve should not read and understand what they have written. But how could they prevent this? It is a dilemma; Diffie – Hellman Algorithm gives solution to seemly difficult distribution of public key exchange problem (ElGamal *et* al., 1985; Menezes *et* al., 1985; Dan, 1988). Diffie – Hellman propounded this sequential explained algorithm:

The first step is for Alice and Bob to agree on a large prime p and a non zero integer $g \bmod p$. The intention of Diffie and Hellman is assumed that the difficulty of the

discrete logarithm problem for F_p^* provides a possible solution.

Haven decided on p and g, Alice and Bob makes these values p and g public knowledge; for example, they might post these values on their web sites. So Eve knows them too.

How to make it difficult for the key to achieve compromise by Brute-force, it is advisable that the choice of g such that its order in F_p^* is a large prime.

Having chosen g and p and make their values public, Alice and Bob make these further decision; Alice picks a secret integer "a" which she can never reveal to anyone including Bob. Also Bob chooses "b" which he keeps to himself. Alile and Bob them make these computation exclusively in their different local dwellings:

$A = g^a \pmod p$

$B = g^b \pmod p$

Alice and Bob then exchange their computations and transmit them through to each other's using the unsecure Internet. Note that Eve gets to see the values of A and B, since they are sent over the insecure communication channel, but he cannot find the discrete logarithms "ä" and "b".

When B get to Alice and A gets to Bob, this further computation is carried out:

$A' = B^a \pmod p$ *and* $B' = A^b \pmod p$

The values of A' *and* B' are actually the same since

$A' = B^a (g^b)^a = g^{ba} = (g^{a)b} = g^{ab} = A^b = B' \pmod p$

We conclude this theoretical algorithm by definition:

Definition 3.1 (Diffie-Hellman Key Exchange)

Let p be a prime number and g an integer. The Diffie-Hellman problem (DHP) is the problem of computing the value of g^{ab} (mod P) from the known values of x $g^b \pmod p$ and $g^b \pmod p$.

1. The ElGamal Public Key Cryptosystem

Diffie – Hellman algorithm provides a method of sharing the key between two parties [6.7,8]. It is, nevertheless, does not provide a full goal of being a cryptosystem. A cryptosystem allows the exchange of specific information and the algorithm for the exchange key. The ElGamal public key encryption is based overwhelmingly on discrete logarithm problems; was developed in 1985 by Taher ElGamal.

The ElGamal public cryptosystem (EPKC) is the first example of PKC; is a number, while the algorithm is the method by which Bob Encrypts his manages using Alice's public key. As we shall see presently, PKC is a number, while the algorithm is the method by which Bob encrypts his messages using Alice's public key. Alice does not disclose her private key which is another number. The private key allows Alice, and only Alice, to decrypt messages that have been encrypted using public key.

2. The EPKC Algorithm

Suppose P is a prime number, and g is a generation of Z_p. The private key x is an integer between 1 and p-2. Assume $y = g^x \bmod p$. The EPKC encryption is the triplet (p, g, y).Suppose further that we take a discrete logarithm and assume it is as difficult as is widely assumed, releasing $y = g^x \bmod p$ does not reveal x. The number x is called an emphemeral key, since it exists only for the purpose of encrypting a single message. Bob takes the plaintext message m, his chosen random ephemeral key x; Alice's public key A and uses them to compute the two equations:

$$\begin{bmatrix} a \equiv g^x \bmod p \\ \\ b \equiv my^x \bmod p \end{bmatrix} \qquad (ElGamal \;\; Encryption)$$

The ciphertext C consists of the pair (a, b) as computed in the Elgamal Encryption. That is C = (a, b).

5.1 The ElGamal Decryption Algorithm

The decryption of the ciphertext C=(a,b) in the ElGamal Scheme, to retrieve the plaintext M is simple:

$$M = \frac{b}{a^x \bmod p} \quad [ElGamalDecryptionAlgorithm]$$

In the above expression, the "division" by a^x should be interpreted in the context of modular arithmetic, that is, M is multiplied by the inverse of $a^x \in Z_p$. The correctness of the ElGamal encryption scheme is easy to verify. Indeed, we have:

$$\frac{b}{a^x} \bmod p \equiv My^k (ax)^{-1} \bmod p$$
$$\equiv Mg^{xk} (g^{kx})^{-1} \bmod p$$
$$= M$$

5.2 Using ElGamal for Digital Signature

Modern Cryptography is concerned not only in encrypting and decrypting of messages. It is also concerned in the authentication of messages sent through the insecured Internet system. The variation of the above scheme provides a digital signature. Namely, a signature for message M is a pair $S = (a,b)$ obtained by selecting a random integer k relatively prime to $p-1$, which of course, equals p and comparing

end
end
n-11
a=powermod(2,n,13); if a==7;
disp(n);

$$\begin{bmatrix} a \equiv g^k \bmod p \\ b \equiv k^{-1}(m - ax)(\bmod(p-1)) \end{bmatrix} \quad (ElGamal\ Signature)$$

To verify a digital signature $s = (a,b)$ we check that

$$g^a a^b \bmod p \equiv ((g^x \bmod p)^a) \bmod p((g^k \bmod p)^{k^{-1}(M-xa)) \bmod (p-1)} \bmod p$$
$$\equiv g^{xa} g^{kk^{-1}(M-xa) \bmod (p-1)} \bmod p$$
$$= g^M \bmod p$$

3. Experimental Examples

The paramount objective of this paper is to clarify through workable numerical examples some models of public-key exchanges exposed above. Based on this, this experimental section is given some practical numerical examples that are established and worked upon for clarify-cation of the models by the Author as seen below and experimented in Matlab.

Example 6.1 (Computing Discrete Logarithm (DL))

This example gives a working example of practical numerical DL:

Find the
$ind_2^{(7)} = 11(\bmod 13)$ *or* $\log_2^{(7)}(\bmod 13)$.

Solution:

For n=1:12;

Therefore, $\log_2^7 = 11(\bmod 13)$

This can be verified by matlab as:

Powermod(2,11,13); such that

ans=7

Example 6.1.1 (Pohlig-Helman Exponentiation Cipher)

Suppose p=263, e=73. Note that the Euler totient value will be $\Phi(n)262$, and Euclidean algorithm gives using the Extended Euclidean algorithm on

Diophantine equation (d=ux+vy) and with Matlab functionality:
Gcd(262,73)=(-61)(73)+(17(262)=1
Since the gcd is 1; a unique solution exist:
[a,b,c]=gcd(73,262)
A=1, b=-61, c=17;
Thus $x = -17 \equiv 201 (\text{mod}\, 262)$
For the cipher text
$c = (246,18,156,0,256,127,18,156,96,256,235,0,132,68)$

which will be decrypted by
$m = f^{-1}(c) = c^d (\text{mod}\, 262)$ (use powermod, for example. (Note: try to use positive d. Using negative d would sometimes cause computation errors)
d=201; p=263; and c[246,18, 156, 0,256, 127, 18, 156, 96 256 235 0 132 68];

m=powermod(c,d) $m = \begin{bmatrix} 19 & 17 & 4 & 0 & 18 \\ 20 & 17 & 4 & 8 & 18 \\ 11 & 0 & 13 & 3 & \end{bmatrix}$

This process gives:

$246^{201} \equiv 19; 18^{201} \equiv 17; 156^{201} \equiv 4; 0^{201} = 0; 256^{201} \equiv 18; 127^{201} \equiv 20; 18^{201} \equiv 17; 156^{201} \equiv 4;$ and
$96^{201} \equiv 8; 256^{201} \equiv 18; 235^{201} \equiv 11; 0^{201} = 0; 132^{201} \equiv 13; 68^{201} \equiv 3$
so the cipher text is:

$(19,17,4,0,18,20,17,4,8,18,11,0,13,3)$,

which means, with Z_{26}, alphabet, the decipherment alphabet, “Treasure Island”.

Example 6.2 (Diffie-Hellman Key Exchange)

Suppose $p = 907,\ a = 2,\ x = 32,\ y = 153.$

Find the exchange key, compute $\bar{x} \equiv 3^{19} = 3$

Solution:

With Matlab functionality computation:

$$xx = power\ \mathrm{mod}(a, x, p)$$

which yields:

$$xx = 311$$

Also:

$$yy = 633$$

Thus

$\bar{x} \equiv 2^{32} \equiv 311;\ \bar{y} \equiv 2^{153} \equiv 633(\mathrm{mod}\,907)$,

as such the common can be calculated by

$k \equiv \bar{x}^{y} (\mathrm{mod}\ p)$

$k \equiv power\ \mathrm{mod}(xx, yy)$

$k = 121$

or by $k \equiv \bar{y}^{x} (\mathrm{mod}\ p)$; such that

$$k = power(yy, x, p)$$

$$k = 121$$

Example 6.3 (ElGamal Cipher)

Suppose A and B are using the ElGamal public-key cipher to communicate with $p = 1231\ and\ e = 15$. Assume furthermore, that A sends a cipher tex $c = (661, 193)$ to B. Find the plaintext m.

Solution:

Here $t = 193\ and\ r = 661$**;** as usual, the matlab computational process obtains:

$r_1 \equiv power\ \mathrm{mod}(r, -e, p)$ which yields:

$$r_1 = 924$$

$$r_2 = \mathrm{mod}(t * r_1, p)$$

Therefore,

$m \equiv t * r^{-e} \equiv 193 * 924 \equiv 21(\mathrm{mod}\,1213)$ **=21**

Thus the message is m=21

Example 6.4 (ElGamal Signature Scheme)

Bob receives $m = 121$ from Alice, together with

$(i)\ sigk(m, r) = (h, g) = (480, 532)\ and$

$(ii) sigk(m, r) = (h, g) = (480, 21)$

Bob downloads Alic's

$$k_E(p, a, b) = (641, 3, 88)$$

which signature should Bob accepts? Which one should he reject?

Solution:

(i) For $sigk(m, r) - (h, g) = (480, 532)$

Bob recognizes that

$b = 88, h = 480\ and\ g = 532$, he computes:

$d = \mathrm{mod}(power\ \mathrm{mod}(b, h\ p) * power\ \mathrm{mod}(h, g, p), P)$

$d = 191$

$m = 121$

$S = power\ \mathrm{mod}(a, m, p) = 350$

Since $s \neq d(\mathrm{mod}\,641)$, this should be rejected.

(ii) For $sigk(m, r) - (h, g) = (480, 21)$

$d = \mathrm{mod}(power\ \mathrm{mod}(b, h, p) * power\ \mathrm{mod}(h, g, p), p) = 350$

$$s = power\ \mathrm{mod}(a, m, p) = 300$$

$$d \equiv s(\mathrm{mod}\,641) = 191$$

Bob accepts it

5.0 CONCLUSION

The theoretical aspects of the paper's models were a bit confusing. With the experimental numerical examples, the work became illuminating, to a layman. The use of Matlab application to aid computational numerical analysis has made the exposure of the paper quite simplified. Thus, with these practical examples, cryptography as a complex mathematical discipline as formerly conceived and established in the classical cryptography is brought down home as a tool for disguising information on the Internet. The practical numerical examples of cryptography as delineated with conspicuous worked practical examples bring bare to any person interesting in

modern cryptography a comprehensive computing conception.

6.0 REFERENCES

ElGamal T. (1985). "A Public-Key Cryptosystems and a Signature Scheme Based on Discrete Logarithms". *IEEE Transactions on Information Theory* **31** (4): 469–472.doi:10.1109/TIT.1985.1057074. .(conference version appeared in CRYPTO '84, pp. 10–18)

Abdalla M. et al (1985). "DHAES, An encryption scheme based on the Diffie–Hellman Problem" (Appendix A).

ElGamal T. (1985). On web: Ä public key cryptosystem and a signature scheme based on discrete logarithms *Advances in cryptology: Proceedings of CRYPTO 84*. Lecture Notes in Computer Science. **196**. Santa Barbara, California, United States: Springer-Verlag, pp. 10–18. doi:10.1007/3-540-39568-7_2.

Menezes A.J. et al. (1985). "Chapter 8.4 ElGamal public-key encryption "Chapter 8.4 ElGamal". *Handbook of Applied Cryptography*. CRC Press. http://www.cacr.math.uwaterloo.ca/hac/about/chap8.pdf

Dan B. (1998). "The Decision Diffie–Hellman Problem". *Lecture Notes in Computer Science* **1423**: 48–63. doi:10.1007/BFb0054851

ElGamal T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm Problem. *IEEE Trans. Info. Theory*, IT-31, 469-472.

Horster P. et al (1994). Generalized El-Gamal Signature Schemes for One Message Block. In *Proc. 2nd Int. Workshop on IT-Security*, 66-81.

Knobloch H.J. (1993). *A Remark on the Size of ElGamal-Type Digital Signatures.* Draft Version.

Lim C.H. et al. (1997). A Key Recovery Attack on Discrete Log Based Schemes Using A Prime Order Subgroup. In *Advances in Cryptology-Crypto'97*, LNCS 1294, Springer-Verlag, 249-263.

Lim C.H. and Lee P.J. (1998). A Study on the Proposed Korean Digital Signature Algorithm. In *Advances in Cryptology-ASIACRYPT'98*, LNCS 1514. Springer-Verlag. 175-186.

Kenneth H. Rose (2006). "Discrete Mathematics and Applications; Cryptography Theory and Practice"; Third Edition; Chapman& Halman/CRC; Taylorand Francis Group; pp1-67

Wenbo M.H-P. (2003). "Company Modern Cryptography: Theory and Practice, Publisher: Prentice Hall PTR" pages: 648.