Lucas Sequence and the Application for Cryptography

Satria Ady Pradana (13510030)
Informatics Engineering
School of Electrical Engineering and Informatics (SEEI)
Bandung Institute of Technology, ITB
Bandung, Indonesia
satria@arc.itb.ac.id

***Abstract*—This paper presents Lucas Sequence and its application for Cryptography. The cryptosystem described here, LUC, is a asymmetric key cryptography which based on Lucas Sequence.**

***Index Terms*—cryptography, asymmetric, lucas sequence, LUC.**

I. Introduction

Nowadays in digital era, information is highly available. Any kind of information, including private information and confidential information, can be obtained using various method. The communication media, such as the internet, has many time prove us how information can be obtained easily.

A protection to confidential and private information is crucial and highly advised. There is no guarantee nor certainty on which attack or leak might occur. Rather than strengthening the security of data storage, protection of data itself would be more effective. Such approach has resulting in cryptography, an art of transforming message (plaintext) into obscured message (ciphertext) which has different meaning or might unreadable.

From ancient time, cryptography has been used especially for military and diplomacy. After invention of digital system and computer, more cryptographic algorithms have been proposed based on computer.

There are dozens and hundreds cryptography algorithms exists. Some of them use simple mechanism such as XOR operation. Some algorithm also take mathematic formula / relation as base. Some unique approach which relies on natural concept such as genetic concept also exists. However all cryptography algorithm can be classified as two categories: symmetric and asymmetric algorithm.

The algorithm described here is using Lucas Sequence as base and can be classified as Asymmetric Cryptography Algorithm. Although being said as cryptography algorithm, it is not a truly algorithm which can replace algorithm like RSA and ElGamal. It serves a purpose as replacement or as alternative of trapdoor function used by other algorithm.

II. Asymmetric Cryptography

Cryptography, is an art and science of writing in secret codes. The name derived from two greek words, kripto which means “hidden” or “secret”, and graphein which means “writing”. In practice, this is the study of techniques for secure communication in the presence of third parties (adversaries or eavesdroppers) and focusing on constructing and analyzing protocols that overcome the influence of adversaries.

There are two operations involved in cryptography: encryption and decryption. An encryption is act or process of encoding message or information which resulting the message unreadable without special knowledge. The decryption is the otherwise, decode the obscured message and read the message.

A cryptography algorithm can be classified into two class: symmetric and asymmetric cryptography. The difference between them is the way a key used for encryption and decryption process.

Asymmetric cryptography, also known as public-key cryptography, is a class of cryptography algorithm which use a set of different keys for encryption and decryption process. Normally there are a pair of key, one key for encryption and the other for decryption. The key for encryption is referred as public key while the key for decryption is referred as private key.

As implied by the name, a public key is key made to be publicly known. Everyone can know this key. Everyone can use this key to encrypt message and send them to the owner of the key. However, one who can decrypt it is only the owner who hold the private key. Yet, private key must be kept only by the owner.

III. Design Principles

Although there are no basic guidelines about how to design an asymmetric cryptographic algorithm, some fundamental principles could be used.

Auguste Kerckhoffs stated design principles for military ciphers [1]. In summary of his definition, a cryptosystem should be secure even if everything about the system (algorithm), except the key, is publicly known. The six design principle stated by Auguste Kerckhoffs are:

1. The system must be practically, if not mathematically, indecipherable;

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;
5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Given the ability of today computers, some principles might irrelevant today. However, the second axiom is still critically important. This means the strength is not determined by the algorithm, which can be public, but the key in which encrypt the message.

In other reference, C.E. Shannon also states two fundamental principles for cryptography algorithm: confusion and diffusion [2].

In Shannon's original definitions, confusion refers to making the relationship between the ciphertext and symmetric key as complex and involved as possible. This principle also includes obscuration of statistic pattern of ciphertext.

The diffusion refers to making the relationship between the ciphertext and the plaintext complex as complex and involved as possible. A single and slight modification might result in unpredicted outcome.

In summary, Shannon states that the relation of both key-message and plaintext-ciphertext should be complex and secure from statistic attack. The principle implies that one cannot find pattern easily and cannot recover plaintext from ciphertext without the key.

IV. LUCAS NUMBERS AND LUCAS SEQUENCE

Lucas numbers are the numbers from Lucas sequence which has similarity to Fibonacci numbers. In other word, it is an instance of Lucas sequence. But moreover, Lucas numbers and Fibonacci numbers form complementary instance of Lucas sequence.

Lucas number is a sequence of integer having recurrence relation to produce a certain term. Each Lucas number is defined to be the sum of its two immediate previous terms. The Lucas number is defined as:

$$L_n := \begin{cases} 2 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ L_{n-1} + L_{n-2} & \text{if } n > 1. \end{cases}$$

If Fibonacci numbers use $F_0 = 0$ and $F_1 = 1$ as base, Lucas number use $L_0 = 2$ and $L_1 = 1$ instead. The first ten terms of Lucas numbers would be:

2, 1, 3, 4, 7, 11, 18, 29, 47, 76

The Lucas number can be extended for negative integer. Using $L_{n-2} = L_n - L_{n-1}$, the negative Lucas number can be obtained for infinite sequence. Following is the extended version of with negative number involved:

…, -11, 7, -4, 3, -1, 2, 1, 3, 4, 7, 11, …

The formula for terms with negative indices in this sequence is

$$L_{-n} = (-1)^n L_n$$

Lucas sequence is an integer sequence. It is a generalization of sequence like Fibonacci numbers, Lucas numbers, and Pell numbers. There are two component $U_n(P, Q)$ and $V_n(P, Q)$ which satisfy following relation:

$$X_n = PX_{n-1} - QX_{n-2}$$

Where P and Q are fixed integer with gcd(P, Q) = 1. Any sequence satisfying this recurrence relation can be represented as a linear combination of the Lucas sequence $U_n(P, Q)$ and $V_n(P, Q)$.

Given two integer P and Q, the Lucas sequence of $U_n(P, Q)$ and $V_n(P, Q)$ are defined by:

$$\begin{gathered} U_0(\mathrm{P}, \mathrm{Q}) = 0, \\ U_1(P, Q) = 1, \\ U_n(P, Q) = P.U_{n-1}(P, Q) - Q.U_{n-2}(P, Q), \end{gathered}$$

$$\begin{gathered} V_0(\mathrm{P}, \mathrm{Q}) = 2, \\ V_1(P, Q) = P, \\ V_n(P, Q) = P.V_{n-1}(P, Q) - Q.V_{n-2}(P, Q), \end{gathered}$$

The initial terms will lead to following sequence (eight terms for $U_n(P, Q)$ and $V_n(P, Q)$ respectively):

n	U_n(P,Q)	V_n(P,Q)
0	0	2
1	1	P
2	P	P^2–2Q
3	P^2–Q	P^3–3Q
4	P^3–2PQ	P^4–$4P^2Q$+$2Q^2$
5	P^4–$3P^2Q$+Q^2	P^5–$5P^3Q$+$5PQ^2$
6	P^5–$4P^3Q$+$3PQ^2$	P^6–$6P^4Q$+$9P^2Q^2$-$2Q^3$
7	P^6–$5P^4Q$+$6P^2Q^2$-Q^3	P^7-$7P^5Q$+$14P^2Q^2$-$7PQ^3$

The relation of $U_n(P, Q)$ and $V_n(P, Q)$ can also be formulated as:

$$U_n(P, Q) = \frac{P.U_{n-1}(P, Q) + V_{n-1}(P, Q)}{2}$$

$$V_n(P, Q) = \frac{(P^2 - 4Q).U_{n-1}(P, Q) + P.V_{n-1}(P, Q)}{2}$$

For n > 1.

A careful inspection would lead to an interesting fact that $U_n(P,Q)$ is Fibonacci numbers for P = 1 and Q = -1 while $V_n(P,Q)$ is a Lucas numbers for P = 1 and Q = -1.

Lucas sequence can be generated over quadratic equations of the form

$$x^2 - Px + Q = 0, P^2 - 4Q \neq 0$$

In which gives following

$$U_n(P,Q) = \frac{a^n - b^n}{a - b}$$
$$V_n(P,Q) = a^n - b^n$$

Where a and b are roots of quadratic equation $x^2 - Px + Q = 0$

$$a = \frac{P + \sqrt{P^2 - 4Q}}{2}$$
$$b = \frac{P - \sqrt{P^2 - 4Q}}{2}$$

The variables a and b, and the parameter P and Q are interdependent. In particular, $P = a + b$ and $Q = ab$. The variable D is defined as discriminant of equation which is $b^2 - 4.a.c$. For every Lucas sequence, there are some theorem which are true:

- $U_{2n} = U_n.V_n$
- $V_n = U_{n+2} - QU_{n-1}$
- $V_{2n} = V_n^2 - 2Q^n$
- $V_{2n+1} = PV_n^2 - QV_nV_{n-1} - PQ^n$
- $V_n^2 = DU_n^2 - 4Q^n$
- $2V_{m+n} = V_mV_n - DU_mU_n$
- $\gcd(U_m, U_n) = U_{\gcd(m,n)}$
- $m|n \rightarrow U_m.U_n \; for \; all \; U_m \neq 1$

In regards of prime natural number, Lucas sequence also holds properties. If p is natural number which is prime number, then

p divides $U_p(P,Q) - \frac{D}{p}$
p divides $V_p(P,Q) - P$

In number theory, Fermat's Little Theorem has big consequences and used for data encryption. It is operation of modular arithmetic and have following

Theorem 1: Given a prime number p and an integer b coprime to p (relatively prime), the congruence $b^{p-1} \equiv 1 \; (mod \; p)$ holds.

The Fermat's Little Theorem can then be seen as a special case of p divides $V_n(P,Q) - P$ because of $a^p \equiv a \; (mod \; p)$ is equivalent to $V_p(a+1, a) \equiv V_1(a+1, a)(mod \; p)$.

V. LUC PUBLIC KEY SYSTEM

LUC is a public-key cryptosystem based on Lucas sequence. LUC itself is implementing the analogs of ElGamal, Diffie-Hellman, and RSA. Instead of using modular exponentiation as in RSA or Diffie-Hellman, encryption of message in LUC is computed as a term of certain Lucas sequence.

In this paper, Lucas sequence will be used as an alternative trapdoor for RSA.

A trapdoor function is a computable function whose inverse can be computed in a reasonable amount of time only if amount of additional information is known / given.

The RSA method use two numbers, e and N, which is formulated as

$$C \equiv M^e (mod \; N)$$

Where M is the message (plaintext) and C is the ciphertext (encrypted message). The chosen number N is the product of two large and different prime numbers, p and q.

The Euler totient function of N, denoted by Φ(N), is the amount of numbers less than N which are relatively prime to N. If N = pq, where p and q are different primes, then Φ(N) = (p-1)(q-1).

The key used for encryption and decryption, notated as e and d respectively, is generated in such e.d = 1 (mod Φ(N)). These e and d are inverse to each other regards on modular Φ(N).

To decrypt message, private key d should be applied to ciphertext.

$$M \equiv C^d (mod \; N)$$

RSA methods works if M is relatively prime to N then $M^{\Phi(N)}(mod \; N)$ is 1. Hence, if M is less than N, $M^{ed} = M^{k\Phi(N)+1} = (M^{\Phi(N)})^k.M = M(mod \; N)$

Using LUC, a different trapdoor function would be defined. Recall the Lucas Sequence

$$X_n = PX_{n-1} - QX_{n-2}$$

Where $\gcd(P,Q) = 1$ and P, Q are integer.

Before going deeper, some definitions should be defined first.

A Legendre symbol is defined as

$$\left(\frac{D}{p}\right) = 0, if \; p \mid D$$
$$\left(\frac{D}{p}\right) = 1, if \; exist \; x \; such \; that \; D \equiv x^2 (mod \; p)$$
$$\left(\frac{D}{p}\right) = -1, if \; no \; such \; number \; exists$$

If p is an odd prime which does not divide Q or D, and ε is $\left(\frac{D}{p}\right)$ then $U_{k(p-\varepsilon)}(P,Q) \equiv 0\ (mod\ p)$ for any integer k, and also $V_{k(p-\varepsilon)}(P,Q) \equiv 2Q^{\frac{k(1-\varepsilon)}{2}}(mod\ p)$.

Lehmer totient function of N = pq, where p and q are different prime numbers, is defined as $T(N) = ((p - \left(\frac{D}{p}\right)(q - \frac{D}{q}))$. Then define $S(N) = lcm(\left(p - \left(\frac{D}{p}\right)\right)\left(q - \left(\frac{D}{p}\right)\right))$.

Since S(N) is a product of both $(p - \left(\frac{D}{p}\right))$ and $(q - (\frac{D}{q}))$ then $U_{kS(N)}(M,1) \equiv 0(mod\ N)$ for any integer k and $V_{kS(N)}(M,1) \equiv 2(mod\ N)$ for any integer k.

Suppose N and e are two chosen numbers with N the product of two different prime numbers, p and q. The e must be relatively prime to $(p-1)(q-1)(p+1)(q+1)$. Let M be a message which is less than N and relatively prime to N. Define $C \equiv V_e(M,1)(mod\ N)$ where V_e is a Lucas function. This will gives ciphertext C.

To define matching private key, a variable d needed to be defined such that $de \equiv 1\ (mod\ S(N))$ where $S(N) = lcm((p - \left(\frac{D}{p}\right)))(q - \left(\frac{D}{p}\right))$ where $D = C^2 - 4$ and $(\frac{D}{p})$ and $(\frac{D}{p})$ are Legendre symbols of p and q. Therefore, D can be assumed as relatively prime to N.

Using extended Euclidean algorithm, number d can be found such that $ed = kS(N) + 1$ for some integer k.

$$V_d(V_e(M,1),1) = V_{de}(M,1) = V_{kS(N)+1}(M,1)$$
$$= MV_{kS(N)}(M,1) - V_{kS(N)-1}(M,1)$$
$$= MV_{kS(N)}(M,1) - \left(\frac{1}{2}\right)\left(V_{kS(N)+1}(M,1)V_q(M,1) - DU_{kS(N)}(M,1)U_1(M,1)\right) = J$$

In this term, J is

$$J \equiv \left(2M - \left(\frac{1}{2}\right)(2M-0)\right)(mod\ N)$$

Which would be the M.

Since $U_{kS(N)}(M,1) \equiv 0(mod\ N)$ for any integer k and $V_{kS(N)}(M,1) \equiv 2\ (mod\ N)$ for any integer k.

Therefore, decryption process would works as:

$$M = V_d(C,1)$$

The choice Q = 1 is not essential for LUC which means it can be any other number. In this term, C could be defined as $C = V_d(M,Q)\ mod\ N$, for some Q depending on the intended recipient who can calculate $V_d(M,Q^e) \equiv V_d(V_e(M,Q),Q^e) \equiv V_{de}(M,Q) \equiv M\ mod\ N$.

VI. Conclusion

LUC use Lucas Sequence as its base for cryptography purpose which has no multiplication.

VII. Acknowledgment

I wish to thank everyone who helped me complete this paper. Without their continued efforts and supports I would have not been able to bring my work to a successful completion.

Dr. Ir. Rinaldi Munir, MT: for guidance and lecture

References

[1] Auguste Kerckhoffs, "La cryptographie militaire" in Jurnal des sciences militaires vol IX, pp. 161–191.
[2] Shannon, C.E. "*Communication Theory of Secrecy Systems*,". 1949.
[3] P.J. Smith, M.J.J. Lennon. "*LUC: A new public key system*". Proceeding of the Ninth IFIP Int. Symposium on Computer Security, pp. 103-117.
[4] P. Ribenboim, "*The New Book of Prime Number Records (3 ed)"*, Springer, 1996.
[5] P. Ribenboim, "*My Numbers, My Friends"*, Springer, 2000.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Mei 2013

ttd

Satria Ady Pradana
13510030