**CAPITULO VI**

En el capítulo V se explicó lo que es un procedimiento de un solo sentido. En este, se estudia el criptosistema asimétrico ElGamal, el cual tiene una función de cifrado que define un proceso de un solo sentido

Iniciaremos nuestro estudio mencionando a los campos finitos de la forma: ; esto es, el conjunto de residuos módulo , con primo [1]. Queda claro que todas las que son diferentes de cero, tienen inverso multiplicativo, ya que mcd.(. Ahora bien, hay algunos elementos que cumplen con el siguiente requisito:

Dado cualquier elemento , tal que , éste se puede expresar de la forma; , donde y . Además, si denotamos al conjunto de todos los residuos sin incluir al cero como ; entonces, podemos observar que el elemento genera todo el conjunto . De hecho, al entero se le llama elemento generador o primitivo del conjunto .

Desafortunadamente no todos los elementos del conjunto son generadores, sin embargo, hay un teorema que nos da la suficiente información para encontrar un elemento generador, dicho teorema se expresa en la siguiente sección.

**VI.1. Cálculo de un elemento generador.**

Teorema 6.1.1. Suponga que es un primo impar diferente de uno. Entonces, se dice que es un elemento generador de , si solo si, , para todo primo diferente de uno que divide a . Esto es, los enteros positivos son los factores primos de

Claramente, del teorema anterior se desprende que el primo se debe construir de tal forma, que sea sencillo factorizar al número , porque la factorización de puede ser compleja. El siguiente teorema nos da una idea de cómo lograrlo.

Teorema 6.1.2. Dados dos enteros positivos tal que son primos relativos. Entonces, es posible construir un número infinito de primos de la siguiente forma: , donde es un entero positivo diferente de cero.

Con base en el teorema anterior nosotros proponemos que , con primos. Además, , donde es un entero positivo. De manera sencilla se puede observar que son primos relativos.

De acuerdo con esta idea, el primo que se construye tendría la forma: . En la práctica el par es un número no mayor a tres cifras, cuando son primos de aproximadamente.

De aquí se sigue que, el número puede factorizase de forma simple. Veamos un ejemplo para ilustrar este punto.

Ejemplo 6.1.1. Dados los primos , construya un primo tal que sea fácilmente factorizable. También, encuentre un elemento generador.

El producto es; 2173. Entonces, para calcular el primo se analizan los enteros de la forma , para , y se elige el más pequeño que sea primo.

, no es primo.

, si es primo.

Se sigue que, . Entonces, los primos que se mencionan en el teorema 6.1.1 son 2, 41 y 53.

El lector puede comprobar que es un elemento generador, utilizando el teorema 6.1.1. Entonces, con este número se puede generar los residuos que van desde 1 hasta 8692. Por otro lado, se señala que estos no aparecen en orden.

Los autores consideran que es conveniente dar un ejemplo con un primo pequeño e ilustrar cuándo un elemento es generador y cuándo no, haciendo todo el desarrollo. Además, ver cómo los valores no aparecen en orden, de hecho, este aspecto es el que le da complejidad a los ataques.

Ejemplo 6.1.2. Suponga que se tiene el primo , por lo que , se sigue que y por lo tanto ; con este valor es posible emplear el Teorema 6.1.1.

Se proponen a , y como posibles elementos generadores, y haremos todos los cálculos para cada caso.

A continuación se escriben todos los ; cuando .

Como puede verse aparecen todos los elementos de , pero en desorden.

Con relación al elemento 4, abajo se presentan los resultados:

Como se observa, el elemento 4 solamente genera los residuos 1, 4, 16 y 13.

**VI.2. El problema del logaritmo discreto.**

Suponga que se tiene la siguiente expresión: ; donde es un número generador, es un primo que se construye de acuerdo al procedimiento de la subsección anterior y es el resultado de la operación modular.

También, considere que se conocen y se desconoce . En este orden de ideas, el cálculo de suponiendo que se conocen los tres parámetros anteriores es muy complejo.

De hecho, este problema se expresa simbólicamente como: , al cual se le llama el problema del logaritmo discreto, ya que es un entero positivo.

En realidad, resolver el problema del logaritmo discreto es más complejo que el problema de la factorización [2].

En este sentido, el criptosistema asimétrico ElGamal se basa en la complejidad de resolver el problema del logaritmo discreto.

En el esquema de comunicación segura de ElGamal, los parámetros son públicos y el valor es privado. También, al entero positivo se le conoce como clave privada.

Por otra parte, el lector se puede percatar que el procedimiento anterior es de un solo sentido o un solo camino.

**VI.3. El criptosistema asimétrico ElGamal.**

Suponga que se construye un primo de al menos 300 dígitos, esto es, su tamaño es del orden El algoritmo de Miller-Rabin se utiliza para proponer dos primos de tamaño cada uno [3], y a partir de estos construir a .

Una vez que se obtiene , se propone un elemento generador, de acuerdo al siguiente procedimiento: se elige un entero positivo . Claramente, el entero positivo seleccionado puede no cumplir con el Teorema 6.1.1, si este es el caso, se propone el entero positivo que le sigue; en otras palabras, .

Nuevamente, se realizan las operaciones señaladas en el Teorema 6.1.1 para averigar si esta nueva propuesta cumple o no con las condiciones de un elemento generador. En caso de que no los cumpla, se propone el que sigue; o sea, . En este punto, seguramente el lector ya se dio cuenta del procedimiento.

La experiencia nos dice que si no es un elemento generador, si lo es algún entero positivo no lejano a . Claro está, siguiendo el procedimiento descrito anteriormente.

Entonces, suponga que se tiene la información que a continuación se escribe: se conocen , tal que . Además, como se mencionó arriba, el primo es de al menos con la finalidad de frustrar ataques, al menos como se llevan a cabo en este momento [4]. Cabe aclarar que, en un esquema de comunicación segura los valores son públicos y es privado.

La función de cifrado para un texto plano, , es la siguiente:

(6.3.1) . Donde:

(6.3.2) .

Se señala que es un entero positivo elegido de manera aleatoria, que cumple con . Por otro lado, la variable se calcula de acuerdo con la ecuación 6.3.3.

(6.3.3)

La función de descifrado, de acuerdo con las variables , es la siguiente:

(6.3.4) .

La demostración de la expresión (6.3.4) no es complicada, a continuación, se presenta los pasos de la prueba:

Sin embargo, y , de acuerdo al pequeño Teorema de Fermat [5]. Por lo tanto, se concluye que:

▄

En algunos libros el proceso de descifrado se realiza de acuerdo con el siguiente procedimiento [5]:

6.3.5.

Sin embargo, el procedimiento anterior tiene la desventaja de calcular el inverso multiplicativo módulo . Se señala que el procedimiento anterior se lleva cabo de forma secuencial lo cual consume más de tiempo, en comparación con el procedimiento de la ecuación 6.3.4. Además, este último puede paralelizarse [6].

En este punto se considera adecuado mostrar un ejemplo, con la intención de aclarar los aspectos descritos anteriormente.

Ejemplo 6.3.1.- Utilizando los datos del ejemplo 6.1.1, suponga que . Entonces, los factores primos de 8692 son: 2, 41 y 53 como se vio en el ejemplo 6.1.1. También, se propone como elemento generador: .

Teniendo en cuenta que , el dato que se desea encriptar, debe cumplir con: Se propone que , y el número seleccionado de manera aleatoria se sugiere que sea . Se sigue que , de donde .

Entonces, el cifrado es: . Donde y . De aquí, y .

En este orden de ideas,

Entonces, el procedimiento de descifrado es:

.

.

. Como se esperaba.

Por otro lado, si realizamos el descifrado mencionado de acuerdo con la ecuación 6.3.5. Entonces, el cálculo de descifrado es como sigue: , el cual da como resultado 100.

Otro aspecto importante que se debe mencionar, es con relación a los ataques a ElGamal. Todos ellos requieren de factorizar al entero . Sin embargo, factorizar a , es equivalente a realizar un ataque al criptosistema RSA.

Recuerde, que la estructura de tiene la forma: . Donde son primos de tamaño .

Entonces, se afirma que atacar al criptosistema ElGamal cuando se construye de la forma anterior se deben resolver dos problemas, a saber:

El primero de ellos es la factorización de , y el segundo corresponde a darle solución al logaritmo discreto.

También, se menciona que el tamaño de los primos que se manejan en ElGamal es menor a los primos que se utilizan en el criptosistema RSA. De hecho, actualmente el valor de en un esquema RSA de alta seguridad es del orden de [7].

Para terminar este capítulo, se menciona que el criptosistema ElGamal se considera aleatorio, por la siguiente razón:

Debido a que las variable de cifrado se construyen a partir del entero que se elige de forma aleatoria, se sigue que cada vez que cifremos un valor, seguramente los valores de serán diferentes. Este tipo de propiedad no la tiene el criptosistema RSA; sin embargo, se puede diseñar un protocolo para aleatorizarlo.

Ejercicios

1. Construya el primo cuando tienen los siguientes valores:

a) y

b) y

2. Encuentre un elemento generador para cada uno de los casos del problema anterior.

3.- Dado un elemento generador, , del problema uno realice los siguientes cálculos:

a) Proponga un valor aleatorio que cumpla con la condición; , y lleve a cabo el cálculo .

b) Plantee un valor para la variable y otro para la clave privada . Con estos datos calcule a y .

4. Utilizando la expresión , descifre el resultado del problema 3.

5. Resuelva el problema anterior de acuerdo con la expresión 6.3.5.

6.- Diga porqué el cifrado de ElGamal se considera aleatorio.

Bibliografía

[1] Gallian J., “Contemporary abstract algebra”, seventh edition, Brooks/Cole, 2011.

[2] HemanthChakravarthy M. and Kannan E., Hybrid Elliptic Curve Cryptography Using Ant Colony Based Authentication System for Cloud Computing, Journal of Engineering and Applied Sciences, 2015.

[3] Stinson R Douglas, Paterson B. Maura. “CRYPTOGRAPHY: Theory and practice”, CRC Press / Chapman & Hall Book, 2020.

[4] Flores-Carapia, Rolando and Silva-Garcia, Victor Manuel and González-Ramírez, MD and Renteria-Márquez, Carlos, A reinforced Elgamal scheme proposal against a pohlig-hellman attack, Applied Mathematical Sciences, Vol. 7, No 59, pp. 2909--2916, 2013, Hikari Ltd.

[5] V. M. Silva–García, R. Flores–Carapia, C. Rentería–Márquez, B. Luna–Benoso, J. C. Chimal–Eguía, IMAGE CIPHER APPLICATIONS USING THE ELLIPTICAL CURVE AND CHAOS, International Journal of applied mathematics and computer science, Vol. 30, 2020.

[6] Murtaza, Abid and Pirzada, Syed Jahanzeb Hussain and Hasan, M Nomam and Xu, Tongge and Jianwei, Liu, “Parallelized Key Expansion Algorithm for Advanced Encryption Standard”, 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), IEEE, pp. 609--612, 2019.

[7] Yarom, Y., Genkin, D. and Heninger, N. (2017). CacheBleed: A timing attack on OpenSSL constant-time RSA, Journal of Cryptographic Engineering 7(2): 99–112.