Ejemplo muy simple de cifrado/descifrado con el algoritmo ElGamal

vtamara@pasosdeJesus.org 24.Jun.2020

Este breve escrito, pretende ayudar a explicar https://es.wikipedia.org/wiki/Cifrado_ElGamal con un ejemplo muy pequeño y simple de generación de llave, cifrado y descifrado. Se precede de unos conceptos mínimos, presentados con gran brevedad sobre aritmética modular.

1. Definiciones previas y propiedades de la aritmética modular

Decimos que un número natural a **divide a** otro número b o que a **es divisor de** b, cuando podemos encontrar un tercer entero n tal que $a \cdot n = b$
Por ejemplo 3 divide a 12 porque $3 \cdot 4 = 12$

Un número entero positivo p es **primo** si sus únicos divisores son 1 y el mismo número.
Por ejemplo 5 es primo porque ni 2, ni 3, ni 4 lo dividen, sólo lo dividen 1 y 5 mismo.

Dado un número natural n llamamos Z_n al conjunto de números naturales $\{0, 1, 2, ..., n\}$ y llamamos Z_n^* al conjunto de números naturales $\{1, 2, ..., n\}$ (es decir sin el 0).
Por ejemplo $Z_5 = \{0, 1, 2, 3, 4, 5\}$ y $Z_5^* = \{1, 2, 3, 4, 5\}$

En Z_n es posible definir operaciones de suma y multiplicación limitadas a Z_n empleando el cociente de la división entre n cuando el resultado de una suma o multiplicación sea n o superior.
Por ejemplo en Z_5 está el resultado de la suma $1+2$ que es 3. Pero no está el resultado de la suma $3+4$ (i.e 7) por lo que se define sacando el residuo al dividir 7 entre 5 que da 2. Eso se denota $(3+4) \equiv_5 2$ que se puede leer $3+4$ es congruente a 2 módulo 5.

Si llamamos $res(a, n)$ al residuo de la división entre a y n, unas interesantes propiedades de la suma y del producto en Z_n es que permiten operar con los residuos, es decir dados a y b números naturales arbitrarios $a + b \equiv_n res(a, n) + res(b, n)$ y también $a \cdot b \equiv_n res(a, n) \cdot res(b, n)$.
Así que las operaciones pueden simplificarse mucho por ejemplo en lugar de hacer multiplicaciones o sumas con números grandes, se pueden hacer con números pequeños modulo n.
Por ejemplo para calcular $111 * 123$ en Z_5 en lugar de obtener el gran producto 13653 para después obtener 3 como residuo de la división entre 5, se pueden primero obtener los residuos $res(111, 5) = 1$ y $res(123, 5) = 3$ y efectuar después el producto $1 \cdot 3$ para concluir $111 \cdot 123 \equiv_5 3$.

Por ser extensiones de las operaciones entre números naturales, la suma así definida cumple las siguientes propiedades (que llamamos propiedades de grupo):

1. Existencia de identidad de la suma, que es el 0 porque para cualquier natural $x \in Z_n$ se da que $(x+0) \equiv_n x$
2. Conmutatividad de la suma porque al sumar 2 operandos pueden ponerse en cualquier orden y darán el mismo resultado (lo que no ocurre por ejemplo con la resta), es decir para cualquier par $x \in Z_n,\ y \in Z_n$ se cumple $(x+y) \equiv_n (y+x)$
3. Asociatividad de la suma porque al sumar 3 operandos, el resultado será siempre el mismo independiente del par de operandos con los que se empiece, es decir para cualquier trío $x \in Z_n,\ y \in Z_n,\ z \in Z_n$ se cumple $(x+y)+z \equiv_n x+(y+z)$ y $(x \cdot y) \cdot z \equiv_n x \cdot (y \cdot z)$
4. Existencia de inversos para la suma, porque dado $x \in Z_n$ al sumarse con $n-x \in Z_n$ dará la identidad de la suma 0. Por lo que el inverso aditivo de x (que se denota $-x$) será $n-x$

También la suma y el producto cumplen la propiedad de distributividad, propiedad que relaciona las operaciones de suma y producto:

5. Distributividad: para cualquier trío $x \in Z_n,\ y \in Z_n,\ z \in Z_n$ se da $x \cdot (y+z) \equiv_n x \cdot y + x \cdot z$

Por su parte el producto en Z_n cumple 3 de las propiedades de grupo:

6. Existencia de identidad de la multiplicación, que es el 1 porque para cualquier natural $x \in Z_n$ se da que $(x \cdot 1) \equiv_n x$
7. Conmutatividad del producto, es decir para cualquier par $x \in Z_n,\ y \in Z_n$ se cumple $(x \cdot y) \equiv_n (y \cdot x)$
8. Asociatividad de la multiplicación, para cualquier trío $x \in Z_n,\ y \in Z_n,\ z \in Z_n$ se cumple $(x \cdot y) \cdot z \equiv_n x \cdot (y \cdot z)$

En los números enteros no hay inversos multiplicativos, como si los hay en los números racionales (donde el inverso por ejemplo de 7 es $\frac{1}{7}$ pues $7 \cdot \frac{1}{7} = 1$ es decir la identidad de la multiplicación).

Pero curiosamente en Z_n^* si hay algunos inversos multiplicativos. Por ejemplo en Z_4 el inverso multiplicativo de 3 es 3 porque $3 \cdot 3 \equiv_4 1$ aunque no haya inverso para 2.

Cuando p es número primo, Dios quiso que Z_p^* tuviera la propiedad de existencia de inversos:

9. Dado $x \in Z_p$ existe un $y \in Z_p$ tal que $x \cdot y \equiv_p 1$ a tal elemento lo denotamos x^{-1} y le llamamos inverso multiplicativo de x

Por ejemplo en Z_5^* los inversos son:

x	x^{-1}	Producto en Z	Producto en Z_5^*
1	1	1	1
2	3	6	1
3	2	6	1
4	4	16	1

Por cumplir esas 9 propiedades con las operaciones de suma y producto definidas, decimos que Z_p con p primo, es un **campo** (como también lo son los racionales, pero no los son los enteros).

Dado que tenemos multiplicación, podemos definir la potenciación para cualquier $x \in Z_p$ así $x^0 \equiv_n 1$ y si a es un entero positivo $x^a \equiv_n x^{a-1} \cdot x$
Que junto con la notación para inversos multiplicativos (en el caso de Z_p) gozará de las propiedades típicas de la potenciación, por ejemplo $x^{a \cdot b} \equiv_n (x^a)^b$ y $x^{a+b} \equiv_n x^a \cdot x^b$ por lo que $x^{-a} \equiv_p (x^{-1})^a$

Tomemos un primo pequeño arbitrario, digamos $p = 5$ por lo que $Z_p = \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ y $Z_p^* = \{1, 2, 3, 4, 5\}$ y calculemos varias potenciaciones:

b	b^0	b^1	b^2	b^3	b^4	b^5	b^6
0	1	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	1	2	4	3	1	2	4
3	1	3	4	2	1	3	4
4	1	4	1	4	1	4	1

Note que las potencias de 0, 1 y 4 se limitan respectivamente a {1,0}, {1} y {1,4}. En cambio las potencias de 2 y de 3 dan {1,2,3,4} así que decimos que 2 y 3 son **generadores** del grupo multiplicativo Z_5^*.

Para cada grupo multiplicativo Z_p^* con p primo, hay generadores y hay bastantes.

2. Ejemplo muy pequeño de cifrado/descifrado con ElGamal

2.1 Generación de llave

Alice debe elegir un primo p (que debería ser grande y tal que p-1 tenga un factor primo grande), un generador g para Z_p^* y generar la llave pública.

Tomemos el primo $p = 5$
De los 2 generadores de Z_5^* eligamos $g = 2$
Como llave privada (que Alice debe mantener en secreto) eligamos $a = 3$

Calculamos $K = 3$ porque $2^3 \equiv_5 3$
Por lo que la llave pública de Alice es $(g, K, p) = (2,\ 3,\ 5)$.

2.2 Cifrado

Para que Bob pueda enviarle un mensaje cifrado a Alice, debe contar con la llave pública de ella.

Digamos que Bob quiere enviarle el mensaje $m = 2$ (un número entre 1 y $p - 1$).
Bob elige y mantiene en secreto un número aleatorio b entre 2 y $p - 1$, digamos que elige $b = 4$
Y calcula el mensaje secreto $(y1,\ y2)$ con:

- $y1 = 1$ porque $g^b \equiv_5 2^4 \equiv_5 1$
- $y2 = 2$ porque $K^b \cdot m \equiv_5 3^4 \cdot 2 \equiv_5 2$

2.3 Descifrado

Alice necesitará su llave pública (g, K, p), su llave privada a y el mensaje cifrado $(y1, y2)$

Con esto, calcula:

$$y_1^{-a} \cdot y_2 \equiv_5 \left(y_1^{-1}\right)^a \cdot y_2 \equiv_5 \left(1^{-1}\right)^3 \cdot 2 \equiv_5 2$$

2.4 Ataque

Un atancante que conozca la llave pública de Alice podría encontrar la llave privada resolviendo para a $g^a \equiv_p K$ que en nuestro ejemplo sería resolver $2^a \equiv_5 3$ que mirando la tabla de potencias da $a = 3$
O en otros términos requiere resolver $log_g(K)$ en el grupo multiplicativo Z_p^*