26/03

Práctico 10: Criptografía

Ejercicio 10. Sean $n = 606409$ y $e = 1111$.

a. Utilizando el esquema de cifrado en bloques ECB para RSA con (n, e), cifrar el siguiente texto

"MATERIA ENLOQUECIDA DE AZAR".

b. Factorizar n mediante el método de Fermat *(ver notas)*.

- $n = p.q$ $\quad p < q$ primos. Queremos determinar p y q.
- para cada $s = 1, 2, 3, \dots$ calculamos $n + s^2$ paramos cuando $n + s^2 = t^2$ ($\square$ perfecto)
- $p = t - s \quad q = t + s$

→ sale de la igualdad: $n = pq = \underbrace{\left(\frac{q+p}{2}\right)^2}_{t^2} - \underbrace{\left(\frac{q-p}{2}\right)^2}_{s^2}$

- $n = 606409$.

$n + 1 = 606410 \rightsquigarrow$ no es cuadrado perfecto.

$n + 4 = 606413 \rightsquigarrow$

$\sqrt{n} \approx 778.7$

$778 \times 778 < n$ ✗

$\underbrace{779 \times 779}_{t^2} = \boxed{606841} \rightsquigarrow$ Queremos ver si la diferencia es cuadrado perfecto.

$t^2 - 606409 = 432$ no es cuad. perfecto

$780 \times 780 = \dots = 1991$ no es cuadrado perfecto.

$\vdots$

$t = 805 \quad s = 204$

$p = 805 - 204 = 601 \qquad q = 805 + 204 = 1009.$

Cifrado ElGamal: El procedimiento de cifrado/descifrado ElGamal se refiere a un esquema de cifrado basado en problemas matemáticos de logaritmos discretos.

Supongamos que Alice quiere comunicarse de manera segura con Bob y lo hace de la siguiente manera. Alice elige un primo p y una raíz primitiva módulo p, luego elige x con $2 \leq x \leq p-2$, y calcula $h \equiv g^x \pmod{p}$. Los datos p, h y g son públicos y x no.

Ahora Bob elige y con $2 \leq y \leq p-2$ y calcula $r \equiv g^y \pmod{p}$. Bob calcula $c \equiv h^y m \pmod{p}$, donde m es su mensaje, y envia r y c a Alice.

Para descifrar Alice calcula $m \equiv cr^{-x} \pmod{p}$.

Ejercicio 9.

a. Explicar por qué funciona el descifrado en el cifrado de ElGamal descripto anteriormente.

b. Si Alice elige los siguientes números $p = 46454609$, $g = 3$, $h = 7902328$ y Bob elige $y = 1142987$ y su mensaje es $m = 7601846$. ¿Cuáles serán los datos r y c que Alice recibe de Bob?

$r \equiv 3^{1142987} (46454609) \equiv 45118009$

$c \equiv 7902328^{1142987} \cdot 7601846 \; (46454609).$

c. Si Bob envía un mensaje a Alice usando el método de ElGamal y de alguna manera obtuvimos el valor y que usó Bob ¿cómo se puede usar ese dato para calcular m?

(a) • Ver que funciona es ver que $m \equiv cr^{-x} \pmod{p}$ (es decir, lo que Alice descifra es el mensaje)

• También tenemos que ver que no cualquiera puede calcular m fácilmente.

• $c \equiv h^y m \; (p)$ (1)
$r \equiv g^y \; (p)$ (2)
$h \equiv g^x \; (p)$ (3)

$$cr^{-x} \overset{(1)}{\equiv} h^y m r^{-x} \; (p) \overset{(2)}{\equiv} h^y m g^{-yx} \; (p) \overset{(3)}{\equiv} g^{xy} m g^{-yx} \; (p) \equiv m \; (p).$$

Idea muy informal

• Si tenemos módulo $n = p$ primo g r.p. y desconocemos x tal que $g \cdot x = a$ ⇝ desencriptar equivale a hallar inversos.

• Si tenemos $n = p$ g r.p. y desconocemos x donde $g^x = a$ ⇒ desencriptar corresponde a resolver un log. discreto (Diffie-Hellman)

• Si tenemos $n = p \cdot q$ y desconocemos d tq $ed \equiv 1 \mod \varphi(n)$ ⇒ el problema es equivalente al de factorizar n. $\exists \varphi(n)$ (RSA)

Obs:

(c) Por (a) $m \equiv c r^{-x} \pmod p$ c y r son públicos.

$c \equiv h^y m \pmod p$

p: es público
h: es público
c: es público
y: lo obtuvimos de alguna manera
m: es privado, lo queremos encontrar.

$m \equiv h^{-y} c \pmod p$ $\Rightarrow$ si tenemos y, hallamos el inverso de $h^y \pmod p$ y lo multiplicamos por c.

Decir para cuáles de los siguientes naturales n existen raíces primitivas módulo n, justificando la respuesta:

- $n = 41$. ✓ (primo)
- $n = 115856201 = 41^5$. ✓ (potencia de primo impar)
- $n = 2 \times 115856201$. ✓ $2 \cdot$(potencia de primo impar)
- $n = 256$. ✗ (potencia de dos)

Teo:
- Si es primo $\Rightarrow$ tiene raíz primitiva
- Si es potencia de primo impar $\Rightarrow$ tiene r.p.
- Si es $2 \cdot$ pot de primo impar $\Rightarrow$ tiene r.p.
- Si es 2 o 4 $\Rightarrow$ tiene r.p.

En otro caso no tiene r.p.