Capítulo 5: Teoría de Números
Clase 2: Criptografía

Matemática Discreta - CC3101
Profesor: Pablo Barceló

¿Qué es la criptología?

La criptología es el estudio de los mensajes secretos.

Uno de sus primeros usuarios fue Julio César: Encriptaba mensajes cambiando cada letra del alfabeto por la letra que está tres veces más adelante.

(Por supuesto, este tipo de encriptación no se considera segura hoy en día).

Formalmente, primero reemplace cada letra por un entero entre 0 y 25.

Luego, encripte mediante la función f que asigna a cada entero $p \in [0, 25]$ el entero $f(p) = (p + 3) \pmod{26}$.

Descifración

Ejercicio: ¿Cómo es posible descifrar un mensaje encriptado de esta forma?

Descifración

Ejercicio: ¿Cómo es posible descifrar un mensaje encriptado de esta forma?

Básicamente usando la función inversa f^{-1} tal que

$$f^{-1}(p) = (p - 3) \pmod{26}.$$

Descifración

Ejercicio: ¿Cómo es posible descifrar un mensaje encriptado de esta forma?

Básicamente usando la función inversa f^{-1} tal que

$$f^{-1}(p) = (p - 3) \pmod{26}.$$

Otras formas un poco más elaboradas:

- Usar para algún entero $k \leq 26$ la función $f(p) = (p + k) \pmod{26}$.
- Usar para algún par de enteros a, b la función $f(p) = (ap + b) \pmod{26}$, de tal forma que f sea una biyección.

Criptografía de llave pública vs llave privada

Todos los métodos anteriores son métodos de llave privada, en el sentido que solo las personas que envían y que reciben el mensaje saben como encriptarlo y descifrarlo.

El problema con esto es que si otra persona se entera de la llave fácilmente puede enterarse de los mensajes.

La llave, por tanto, tiene que ser cuidadosamente intercambiada.

Criptografía de llave pública vs llave privada

En los sistemas de llave pública, cualquier persona conoce la llave para encriptar el mensaje, no así para descifrarlo.

La llave para descifrarlo se mantiene privada, y no necesita ser intercambiada.

Sabiendo la llave de encriptación es posible obtener la llave para descifrar, pero al costo de ocupar recursos computacionales imposibles (2 millones de años, por ejemplo).

Criptografía RSA

Desarrollada por Rivest, Shamir y Adleman en 1976 (les valió el Turing award el 2003).

También inventada en paralelo, pero en secreto, en el gobierno norteamericano, en 1973 por Clifford Cocks.

La clave de encriptación es de la forma (n, e), donde $n = pq$, para p y q primos *grandes*, y e es un primo relativo a $(p-1)(q-1)$.

Encontrar dos primos *grandes* es fácil usando técnicas probabilistas, e.g. test de Miller-Rabin.

Sin embargo, si un adversario solo ve n es computacionalmente *difícil* que lo factorice para encontrar el par (p, q).

Encriptación RSA

Asumimos que el mensaje M está dado como una secuencia de enteros (sino tan solo lo transformamos en un mensaje de esta forma).

Luego, computamos el valor $C = M^e \pmod{n}$.

Esto es relativamente fácil de hacer utilizando algoritmos para exponenciación modular.

Pregunta: ¿Se le ocurre cómo funcionan estos algoritmos?

Llave descifradora

La llave descifradora d es cualquier entero tal que

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Ejercicio: Demuestre que un entero d como se define arriba siempre existe.

Descifrando en RSA

Ahora mostramos cómo descifrar C usando d.

Sabemos que existe entero $k \geq 0$ tal que:

$$de = 1 + k(p-1)(q-1).$$

Por tanto,

$$C^d \equiv (M^e)^d \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

Descifrando en RSA

Note que raramente p o q dividirán a a, y por tanto, por el pequeño Teorema de Fermat: $M^{p-1} \equiv 1 \pmod{p}$ y $M^{q-1} \equiv 1 \pmod{q}$.

Concluimos que

- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \pmod{p}$, y
- $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \pmod{q}$.

Por tanto, $C^d \equiv M \pmod{pq}$. (¿Por qué?)

¿Cómo funciona?

La clave pública está disponible para mandarle mensajes al receptor, pero la privada la mantiene el receptor sin publicarla y la utiliza para descifrar.

Es fácil encontrar d desde e solo si se conoce una factorización prima pq de n.

En caso contrario, hay que encontrar factorización prima, lo que es algo costoso. (Actualmente no se sabe cómo factorizar números de más de 100 dígitos).