Pequeña introducción a la criptografía

Daniel de Roux

8 de Agosto de 2015

Objetivo:

El objetivo de este trabajo es dar introducir el material que vamos a necesitar para entender el funcionamiento de los bitcoins. Ninguno de los temas tratados es complicado.

Temas

- Criptografía de clave simétrica
- criptografía de clave pública
- clave digital

Motivación.

Por qué necesitamos la criptografía de clave pública? Cuales son sus ventajas?

Criptosistema

Definición (Criptosistema)

Un criptosistema es un tupla (P, C, K, E, D) *donde:*

- P *es un conjunto finito de tecto*
- C *es un conjunto finito de tecto cifrado*
- K *es el espacio de llaves*
- $\forall k \in K$ *eciste un protocolo de encripatación* $e_k \in E$ *y una regla de desencriptación* $d_k \in D$.
- *Cada* $e_k : P \to C$ *y* $d_k : C \to P$ *son funciones tales que* $d_k(e_k(x)) = x \ \forall x \in P$.

Ejemplo

Criptosistema de Cesar
Tomamos $P = C = K = \mathbb{Z}_{26}$ Tomamos $k \in K$.

$$e_k(x) = x + k \ mod(26)$$

$$d_k(y) = y - k \ mod(26)$$

Es este criptosistema seguro? Hablemos de AES.

Criptosistema de clave pública

La seguridad de RSA se basa en la dificultad de factorizar números grandes en sus componentes primos. Este problema no tiene solución en tiempo polinomial para números de b-bits grandes. (si logramos desarollar la computación cúantica, existe un algoritmo que resuelve este problema en $O(b^3)$.

One way function

La idea de un criptosistema a clave pública es que sea dificil determinar d_k dado e_k. Es decir, e_k debe ser una on way function.

Definición

Una one way function es una funcíon fácil de computar pero difícil de invertir.

Ejemplo : sea b un entero positivo y n un entero producto de dos primos grandes. $f : \mathbb{Z}_n \to \mathbb{Z}_n$

$$f(x) = x^b \ mod(n).$$

Esta función es problablemente una one way function.

RSA

Sean p y q primos impares. $n = p.q$, notemos que $\phi(n) = (p-1)(q-1)$.
$P = C = \mathbb{Z}_n$.

$$K = (n, p, q, a, b) : ab \equiv 1 \ mod \phi(n))$$

$$e_k(x) = x^b \ mod(n)$$

$$d_k(y) = y^a mod(n)$$

Los valores n, b son la clave pública, p, q, a son la clave privada.

RSA

Sabemos que

$$ab \equiv 1 \ mod(\phi(n))$$

Entonces

$$ab = t.\phi(n) + 1$$

$$(x^b)^a \equiv x^{t.\phi(n)+1} \ mod(n)$$

$$x^{ab} \equiv x^{t.\phi(n)}x \ mod(n) \equiv x \ mod(n)$$

Ejemplo

Bob pone $p = 101,\ q = 113$ entonces n=11413. $\phi(n) = 100.112 = 11200$
$11200 = 2^6.25^2.7$ Así que b no debe ser divisible por $2, 5, 7$. Por ejemplo, $b = 3533$ y $b^{-1} mod(11200) = 6595$ Así que $a = 6597$.
Bob publica $n = 11413, b = 3533$. Alice quiere encriptar 9726.

$$9726^{3533}\ mod(11413) = 5761.$$

y

$$5761^{6597}\ mod(11413) = 9726.$$