Funciones de un sólo sentido

José Galaviz

El problema de la criptografía

- A lo largo de la historia uno de los problemas centrales de la criptografía es el de distribuir la clave.
- No es posible usar el canal intervenido.
- Es necesario salir del sistema criptográfico para lograr que emisor y receptor tengan la clave.

¿Cuál es el problema?

- Repartir la llave usando un canal inseguro, o…

¿Cuál es el problema?

- Repartir la llave usando un canal inseguro, o…
- Lo que queremos realmente es tener manera de enviar mensajes cifrados al destinatario sin que el espía los pueda leer y sin tener que decirnos ninguna clave que se lo permita.

¿Se les ocurre algo para resolver el problema?

Solución

- Que haya dos claves: una para cifrar y otra para descifrar.
- Dado un usuario X
  - Una (e) para cifrar mensajes dirigidos a X que todo mundo puede conocer.
  - Una (d) para descifrar los mensajes que van dirigidos a X y que sólo posee X.
- Aún conociendo e y el algoritmo de cifrado, no tengo lo necesario para descifrar.

Funciones

- Si lo pensamos como la aplicación de una función:
  - $F(e, M) = S$
  - Sólo el destinatario puede calcular $F^{-1}(e, M) = F(d, S)$ fácilmente.
- Es sencillo calcular la función.
- Es difícil calcular la inversa.

Funciones de un sentido (One Way Functions)

- Concepto puramente computacional.
- Es fácil calcular la función en un sentido.
- Es difícil hacerlo en sentido contrario.
- Como un rompecabezas.

Función de un sentido

- Fácil desarmarlo.
- Difícil armarlo.

Mensaje escrito al reverso

El espía tarda mucho en armarlo…

Función de un sentido

- Fácil desarmarlo.
- Difícil armarlo.

Mensaje escrito al reverso

El espía tarda mucho en armarlo…

También el destinatario

Funciones de puerta de trampa (Trapdoor Functions)

Haya un elemento adicional que al conocerlo el destinatario, le haga fácil la tarea.

- Un patrón de armado.
- La clave de descifrado.

Concepto computacional

- En matemáticas las funciones son invertibles o no lo son.
- Los conceptos de one way function y trapdoor function son puramente computacionales.
- Se refieren a la dificultad de calcular algo.

El catálogo de Comex

One way function

- Es sencillo tomar los colores básicos: rojo, azul, amarillo, blanco y negro, definir una proporción exacta de ellos y mezclarlos para generar un color C del catálogo.
- Dado un color del catálogo, sin saber nada más, es muy difícil generar exactamente el color C adivinando las proporciones exactas de los colores básicos a mezclar.

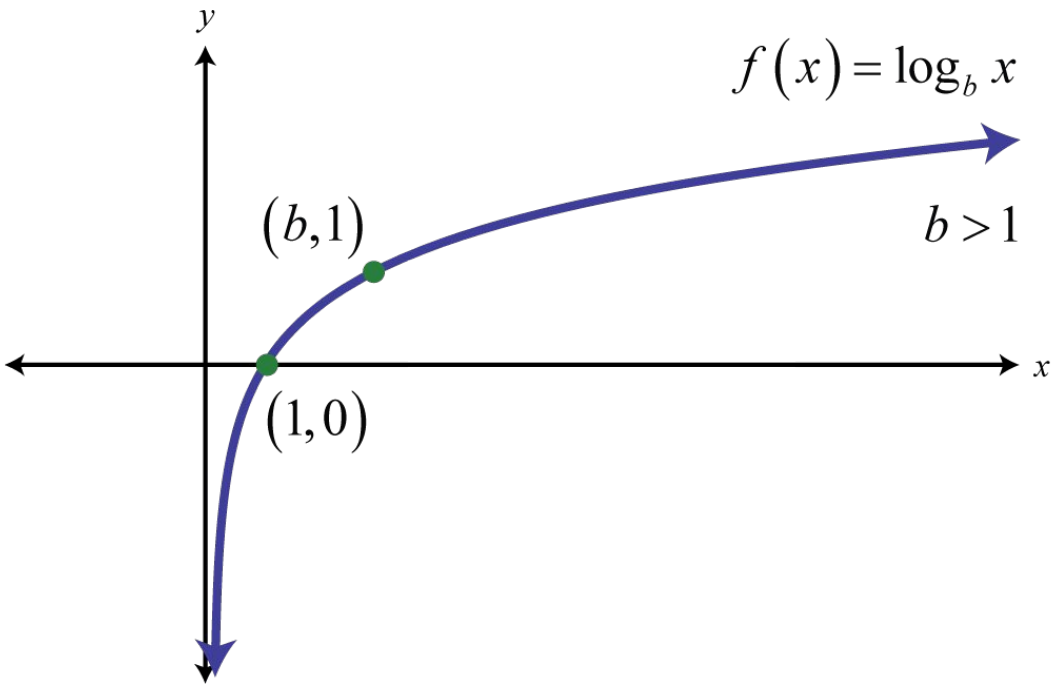
Video

¿Y hay problemas verdaderos?

- El problema del logaritmo discreto.
- El problema de la factorización.

El logaritmo

- Si $x = b^y$, y es el logaritmo de x en base b.
- $y = \log_b x$
- Tiene sentido siempre que b, $x > 0$ y $b \neq 1$.



Pero no sólo están los reales

- Hay otros conjuntos (grupos, campos finitos) en los que el logaritmo tiene sentido.
- Por ejemplo (caso simple), en los enteros módulo un número primo p.

Pero…

- Puede no existir.
  - No existe ningún número n tal que $2^n = 6$ en los enteros módulo 7.
  - 2^n sólo puede ser congruente con 1, 2 y 4 módulo 7
- Es tanto más difícil de calcular cuanto mayor sea el tamaño del módulo.

El problema de la factorización

- Dados dos o más números primos p_1, p_2, …, p_k.
- Es simple obtener el producto de ellos

$$N = p_1\, p_2 \ldots p_k.$$

- Pero dado N es muy difícil determinar los primos cuyo producto es N.
- Sabemos que existen y son únicos salvo el orden.
- Encontrarlos no es trivial si el tamaño de N es muy grande.

¿Cómo usamos estos problemas?

Ya veremos...