CRIPTOGRAFÍA

En efecto, Histieo, que deseaba incitar a Aristágoras a rebelarse, en vista de que los caminos se hallaban vigilados, sólo encontró un medio para transmitirle el encargo con garantías de éxito: afeitarle totalmente la cabeza al más leal de sus esclavos, tatuarle un mensaje, y esperar a que le creciera nuevamente el pelo; y, en cuanto le creció lo suficiente, lo envió a Mileto, dándole como única orden que, una vez llegado a Mileto, indicase a Aristágoras que le afeitara el cabello y le echase una ojeada a la cabeza (los signos tatuados incitaban, como ya he señalado antes, a la rebelión).

Libro V de la Historia de Heródoto

Sistemas criptográficos sencillos

Según Suetonio, Julio César utilizaba el sistema criptográfico que consiste en desplazar tres posiciones cada letra del alfabeto:

$$BUENOS\ \ DIAS \rightarrow EXHPRV\ \ GLDV$$

Sistemas criptográficos sencillos

Según Suetonio, Julio César utilizaba el sistema criptográfico que consiste en desplazar tres posiciones cada letra del alfabeto:

$$BUENOS\ DIAS \rightarrow EXHPRV\ GLDV$$

Podemos desplazar las letras tantas posiciones como queramos y podemos expresar el proceso de cifrado matemáticamente:

Identificando $\{A, B, C, D, \dots\}$ con $\{0, 1, 2, 3 \dots, 26\}$,

$$E(x) \equiv x + c \bmod 27$$

$$D(x) \equiv x - c \bmod 27$$

c es la clave de cifrado, pero ¡es muy fácil romper el código!

Ejemplo de mensaje con cifrado César

VÑ QKC NÑCMELRÑBDY

Se puede complicar un poco si en lugar de una clave, usamos dos:

$$E(x) \equiv ax + c \bmod 27$$

$$D(x) \equiv a^{-1}(x - c) \bmod 27$$

Hace falta que $mcd(a, 27) = 1$. ¿Por qué?

Se puede complicar un poco si en lugar de una clave, usamos dos:

$$E(x) \equiv ax + c \bmod 27$$

$$D(x) \equiv a^{-1}(x - c) \bmod 27$$

Hace falta que $mcd(a, 27) = 1$. ¿Por qué?

Pero sigue siendo fácil romper el código. ¿Sabéis por qué?

Otro ejemplo: descubrid las claves a y c.

VEVJVOSBIR, JR QVBI HBSNTO

¡Atención!: Es un mensaje en inglés, con un alfabeto de 26 letras.
La letra más frecuente en inglés es la E, seguida de la T y la A
Claro que este mensaje es muy cortito, pero ¿quién sabe?

Podríamos, para complicar las cosas, realizar una permutación arbitraria de las letras del alfabeto.

Pero sigue siendo bastante fácil romper el código cuando hay un mensaje coherente: ¿Por qué?

John Lennon

KP WEGP QJ PLVQKKN LVQ YQ WP

JVXQGEQBGN ZEQBYIPJ YQ QZUQSPJ QB

FPXQI NYINJ UKPBQJ.

Algunas ideas más complejas

Probemos entonces a no hacer una permutación de las letras del alfabeto... Busquemos algo más complejo:

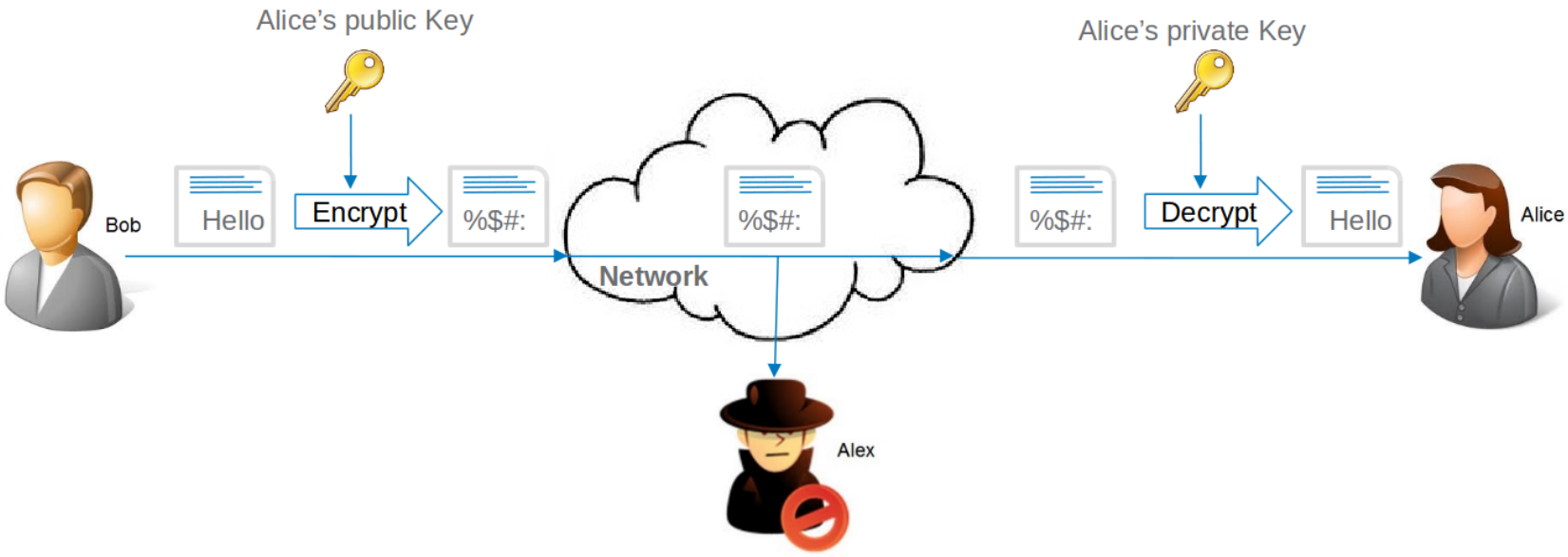
- Cifrado Hill (1929): la clave es una matriz.

  Aquí hay un ejemplo.
- Máquina Enigma: las claves son permutaciones.
  Lo explican más esquemáticamente Aquí.

  Para entender cómo consiguieron descifrar el código es importante saber algo de Teoría de Grupos.

Problema común: son sistemas simétricos, de clave privada. Es necesario realizar un intercambio de claves.

Clave pública



https://www.binderror.com

RSA: Rivest, Shamir, Addleman (1977)

Como usuario del sistema RSA, tengo dos claves, una pública y otra privada. Para construir mis claves procedo de la siguiente manera:

1. Busco dos números primos distintos p y q, grandes, de al menos 300 dígitos.
2. Calculo $n = pq$.
3. Calculo $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+q) + 1$.
4. Elijo $e \in \{1, \ldots, \varphi(n) - 1\}$ tal que $mcd(e, \varphi(n)) = 1$.
5. Calculo $d \in \{1, \ldots, \varphi(n) - 1\}$ inversa de e mod $\varphi(n)$, esto es,

$$ed \equiv 1 \bmod \varphi(n).$$

Mi clave pública será el par (e, n) y mi clave privada va a ser (d, n).

Encriptación con RSA

Cuando alguien quiera enviarme un mensaje, lo primero que tendrá que hacer es convertirlo en un número, llamémosle $M \in \mathbb{N}$.
Se puede hacer asignando a cada símbolo del mensaje su código ASCII,

$$HOLA \to [72, 79, 76, 65],$$

y entonces, por ejemplo:

- $M = 72797665$ o 072079076065
- $M = 72 \cdot 256^3 + 79 \cdot 256^2 + 76 \cdot 256 + 65 = 1213156417$

A continuación, buscará mi clave pública, (e, n), y me enviará el resultado de la siguiente operación:

$$M' = M^e \bmod n.$$

Cuando yo reciba el mensaje encriptado M', realizaré la misma operación que para el encriptado, pero con mi clave privada:

$$M'' = M'^d \bmod n.$$

Como

$$M'' \equiv M'^d \equiv (M^d)^e \bmod n$$

y $de \equiv 1 \bmod \varphi(n)$, entonces $M'' \equiv M \bmod n$.

Si el número M es menor que n, habré recuperado íntegramente el mensaje original.

Algunas consideraciones

- El teorema de Euler es cierto cuando $mcd(M, n) = 1$.
- $M < n$.
- ¿Por qué es difícil romper la clave?
  - Calcular $\varphi(n)$ es tan complejo como factorizar n.
  - Dificultad para factorizar: RSA numbers.
  - Algoritmo polinomial de Shor (ordenador cuántico).
- A menudo se usa el sistema RSA no para encriptar el mensaje completo, que es largo, sino simplemente para compartir claves. En este enlace se explica por qué y se indica que para encriptar los textos es más rápido un algoritmo simétrico como Advanced Encryption Standard (AES).

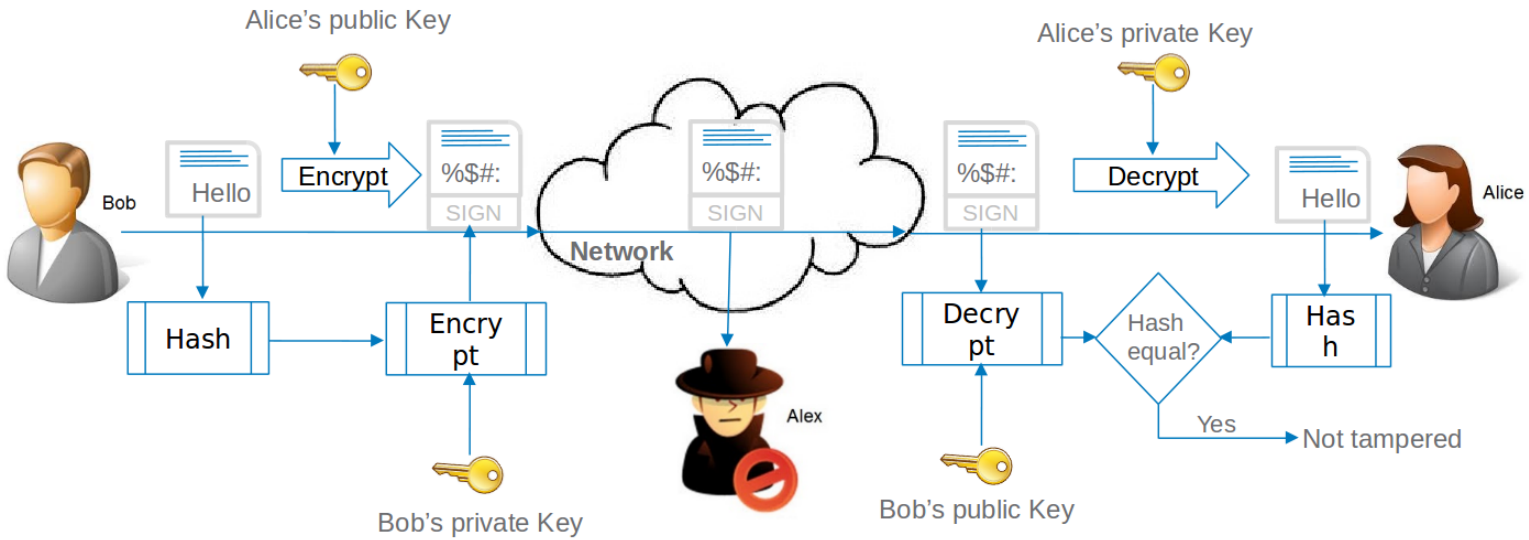
Firmas

La Fábrica de Moneda y Timbre expende estos certificados electrónicos para firmar digitalmente:

El firmante encripta su mensaje con su clave privada y el receptor desencripta con la pública.

El texto firmado por el certificado digital, cuando firmamos, es un resumen realizado por una función hash. En este documento explican los detalles.

En este documento de la FNMT se citan los algoritmos que utilizan sus tarjetas criptográficas. Como algoritmos de clave pública utiliza, además de RSA, el de Curvas elípticas.



https://www.binderror.com

Hay otros sistemas criptográficos, que se han usado menos que el RSA, pero que también son interesantes, como el del **logaritmo discreto** o los que usan **curvas elípticas**. No los hemos mostrado porque requieren aprender más matemáticas.

En el taller comentamos que RSA es un buen método criptográfico porque la factorización de números enteros en producto de primos es una tarea muy complicada computacionalmente, pero que existe un algoritmo, el **algoritmo de Shor**, que lo realizaría de forma eficiente en ordenadores cuánticos.