CRIPTOGRAFÍA

Metodos de Cifrado

1- Metodo Cesar

Fijada una clave $K \in \mathbb{N}$, le sumamos a cada letra la clave K y reducimos modulo 28

2- Metodo Afin:

Fijada una clave $\ell = (a, k)$ con $a \in U(28)$ y $K \in \mathbb{Z}_{28}$, le aplicamos la función $E(x) = ax + K \mod 28$ a cada letra.

Para deleneriptar aplicamos $D(y) = (y - k) \cdot a^{-1} \mod 28$

3- Metodo Vigenere

La clave fijada es una secuencia de palabras. Sumamos cada letra al texto puano y reducimos mod 28

Metodo de intercambio de clave privada

Metodo Diffie-Hellman

a) Se elige un primo p y g raiz primitiva de p

b) Persona 1 elige $n \in \mathbb{N}$, calcula $a \equiv g^n \mod p$ y se lo envia a la Persona 2

c) Persona 2 elige $m \in \mathbb{N}$, calcula $b \equiv g^m \mod p$ y se lo envia a la Persona 1

d) Persona 1 delencripta calculando $k \equiv b^n \mod p$
Persona 2 delencripta calculando $k \equiv a^m \mod p$

CRIPTOSISTEMAS DE CLAVE PUBLICA

(Por más que se conozca el cifrado no es facil saber el decifrado)

RSA:

a) Se eligen 2 primos p y q ($p \neq q$) y se calcula $n = p \cdot q$

b) Se calcula $\varphi(n)$

c) Se elige $e < \varphi(n)$: $\mcd(e, \varphi(n)) = 1$

Función de Cifrado:
$E(x) = x^e \mod n$, siendo (n,e) publico

Función de decifrado
$D(y) = y^d \mod n$

Con d = inverso de e mod $\varphi(n)$
$d \cdot e \equiv 1 \mod \varphi(n)$

Proposición:
Sean p, q, n, d y $e \in \mathbb{Z}$ tales que $e \cdot d \equiv 1 \mod \varphi(n)$ y las funciones $E(x) = x^e \mod n$ y $D(y) = y^d \mod n$
Entonces:
$D(E(x)) \equiv x \mod n$

Metodo de Fermat

Sea $n = p \cdot q$ con $p < q$
Para $s = 1, 2, \ldots$ calculamos $n + s^2$ y paramos cuando no es un cuadrado perfecto ($n + s^2 = t^2$ con $t \in \mathbb{Z}^+$)
Entonces:
$p = t - s$ y $q = t + s$