Criptografía: disciplina que estudia metodos para proteger datos frente a adversarios, es decir, protege los datos en cuanto a la privacidad

Objetivo: la criptografía moderna no busca metodos imposibles de romper, si no sistemas imposibles de romper en la practica con los recursos computacionales actuales

- Criptografía clásica o antigua (Antes del siglo XX)
  - Basado en el secreto del método (transposiciones, sustituciones)
  - No tiene un fundamento matemático solido
- Criptografía moderna (siglo XX para adelante)
  - Basado en modelos matemáticos formales y la teoría de la complejidad informática

Ejemplos de criptografía clásica

- Cifrado cesar: las letras se desplazan 3 lugares considerando el abecedario

ej. A → D
B → E
⋮

ATAQUE ⇝ DWDTXH

Investigar que pasaba con los espacios en blanco

Generalización: se desplazan n en lugar de 3

- Cifrado Vegenere

Clave: "Clave"

Texto Hola

Textro Cifrado
JZLV

H (7)	C (2)	9 (5)
O (14)	L (11)	25 (Z)
L (11)	A (0)	11 (L)
A (0)	V (21)	21 (V)

Para romper
1) Determinar la long de la clave
2) Poner el texto cifrado en una matriz de 3 columnas

C1	C2	C3
⋮	⋮	⋮

se aplica el metodo p/ romper el codigo césar

Criptografía moderna

- Un sist. criptografico moderno es computacionalmente seguro si romper el sistema es inviable computacionalmente

- Principio de KercKhoffs: el sist. criptográfico debe ser seguro si todo, excepto la clave, es conocida

Criptografía simetrica: Clave compartida

Criptografía asimetrica: (de clave publica) $\begin{cases} \text{clave publica} \\ \text{clave privada} \end{cases}$

Esquema de criptografía simetrica

Texto plano
⇝ se cifra con clave K
⇝ texto cifrado
⇝ se descifra con clave K
⇝ texto plano

Esquema de clave publica

Texto plano
⇝ se cifra con la clave publica
⇝ texto cifrado
⇝ se descifra con la clave privada
⇝ texto plano

| Investigar sobre firmas digitales |

Ejemplos de cifrados simetricos

- DES (obsoleto) } cifrado por bloque
- AES
- Chacha 20 cifrado por flujo

⋮

y muchos mas

Ventajas: rapido, simple, eficiente para grandes volumenes de datos

Desventajas: manejo de la clave compartida

Ejemplos de criptografía de clave publica

- RSA
- El Gramal (basado en la factorización de enteros)
- De curvas Elipticas (basado en el problema de logaritmo discreto)

① RSA (Rivest, Shamir, Adleman, 1977)

↳ aritmetica modular: ej "modulo 7" $\{0;1;2;\dots;6\}$

$5+6=11\equiv 4 \pmod 7$

$5\cdot 6=30\equiv 2 \pmod 7$

- propiedad multiplicativa inversa

x	y	x·y
1	1	1
2	4	1
3	5	1
4	2	1
5	3	1
6	6	1

- propiedad exponencial

Fermat/Euler $a^6 \equiv 1 \pmod 7$

$\neq 0$

ejemplo de modulo 6: $\{0;1;2;\dots;5\}$

x	y	x·y
1	1	1
~~2~~		
~~3~~		
4		
5	5	1

como 6 no es primo, y esta compuesto por dos n° primos los multiplos de essos dos numeros "2" y "3" no aparecen en la tabla

Funcionamiento de RSA

1. se toman 2 numeros primos
2. se calcula $n = p \cdot q$
3. se calcula $\varphi(n) = (p-1)(q-1)$
   (función ε de Euler)
4. se elige un numero entero que satisface
   $$\begin{cases} 1 < e < \varepsilon(n) \\ \text{mcd}(e, \varepsilon(n)) = 1 \end{cases}$$
5. se calcula d tal que $e \cdot d \equiv 1 \pmod{\varepsilon(n)}$
6. la clave privada es (n, d), la clave publica es (n, e)

__Cifrado__ texto plano m

$$c \equiv m^e \pmod{n}$$

__Descifrado__

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{\varepsilon(n) \cdot x + 1} \equiv (\underbrace{m^{\varepsilon(n)}}_{\equiv 1})^x \cdot m \pmod{m}$$

$$\equiv m \pmod{m}$$

Ejemplo:

1. $p = 7 \quad q = 11$
2. $n = 77$
3. $\varepsilon(n) = 60$
4. tomamos $e = 17$
5. $53 \cdot 17 = 901 = 900 + 1 = 60 \cdot 15 + 1$
   $\rightsquigarrow 53 \cdot 17 \equiv 1 \pmod{60} \rightsquigarrow d = 53$
6. cl. publica $(77, 17)$
   cl. priv $(77, 53)$

* __cifrado__ $m = 20$

$$20^{17} = 20 \cdot 20^{16} = 20 \cdot \left(\left(\left(20^2\right)^2\right)^2\right)^2$$

$20^{17} = 20^{10} \cdot 20^7 = 1 \cdot 48$ mod 77

n	20^n
1	15
2	$69 \equiv -8$
3	$20 \cdot (-8) \equiv -6$
4	$20 \cdot (-6) \equiv 34$
5	$(-8)^2 \equiv 64 \equiv -13$
6	$(-8) \cdot (-6) \equiv 48 \equiv -19$
7	$(-6)^2 = 36$
8	

* __Descifrado__ $(48)^{53} \equiv ? \bmod 77 \rightarrow 20$

Curvas elipticas

(sobre $\mathbb{R}$)

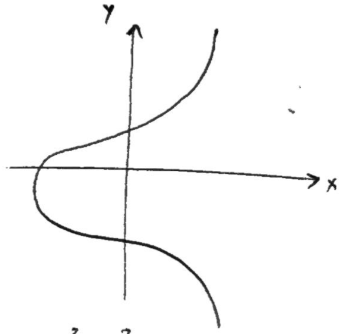
Una curva eliptica es una curva dada por la ecuación de Weierstrass

$$E: \quad y^2 = x^3 + ax + b$$

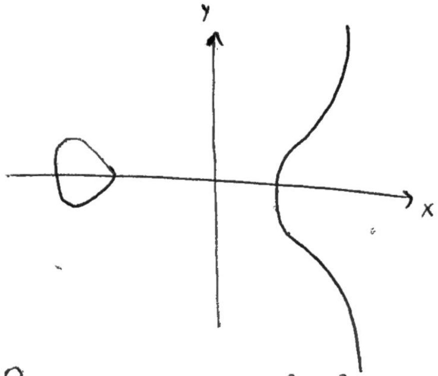
donde $a, b \in \mathbb{R}$ y el discriminante

$$\Delta = -16\,(4a^3 + 27b^2)$$

es distinto de cero

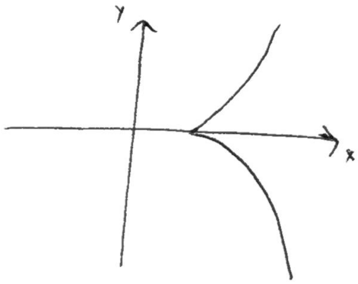


$y^2 = x^3 - x + 1$

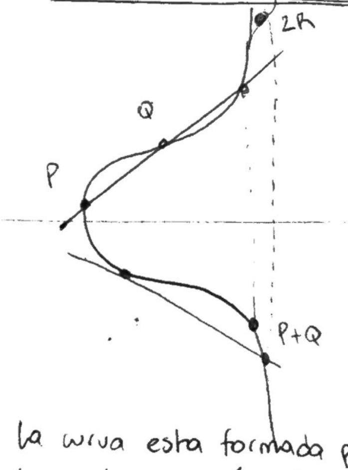


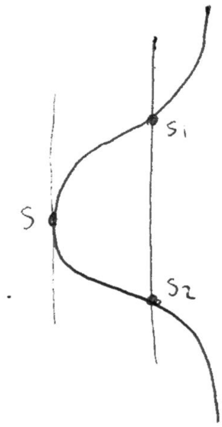
$y^2 = x^3 - x$

si $\Delta = 0$



la "suma" geometrica





$S_1 + S_2 = \infty$ = "0" (cero)

$\hookrightarrow S_2 = -S_1$

$2S_2 = 0$

$\hookrightarrow -S = S$

la curva esta formada por las soluciones (x, y) de W mas el punto "infinito"

(es el cero del grupo de la curva)

La "suma" algebraica

$P \neq Q$; $P(x_1; y_1)$; $Q(x_2; y_2)$

pendiente $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$ $\qquad P+Q = (x_3; y_3)$

cuando $P = Q \rightsquigarrow \lambda = \dfrac{3x_1^2 + a}{2y_1}$

PLD : Problema de logaritmo discreto

$\left.\begin{array}{l} \text{tomo } P \text{ en la curva (pública)} \\ \text{tomo } n \in \mathbb{Z}_+ \text{ (privado)} \\ \text{calculo } Q = n \cdot P \text{ (público)} \end{array}\right\}$ imposible calcular n

(teoricamente se puede pero tarda demasiado)

notacion multiplicativa

$P^n = Q$

se debe aplicar logaritmo pero no se puede resolver

$\boxed{\text{investigar más sobre ~~toga~~ problemas de logaritmo discreto}}$