

Evolució de la criptologia

Perquè és el moment de les Corbes El·líptiques

Sergi Blanch i Torné

Matemàtica Discreta, Criptografia i Anàlisi de dades
Escola Politècnica Superior
Universitat de Lleida

V Jornades de Programari Lliure
Juliol 2006

Index

- 1 Introducció
- 2 Criptosistemes clàssics
- 3 Criptosistemes mecànics
- 4 Criptosistemes computacionals

Què és la criptologia?

Definim

Criptologia com l'estudi de les tècniques matemàtiques relatives a la seguretat de la informació.

- Criptografia: Produeix criptosistemes segurs.
- Criptoanàlisi: Trenca els criptosistemes.
- Esteganografia.

Què volem de la criptologia?

Definim

Criptologia com l'estudi de les tècniques matemàtiques relatives a la seguretat de la informació.

- Confidencialitat: ocultar d'ulls indiscrets.
- Integritat: alteracions no autoritzades.
- Autenticació: identificar la procedència.
- No-rebuig: negar l'emissió.

Teoria de la Informació

Segons Claude E. Shannon:

“Un bon xifrat ha d'aplicar *confusió* i *difusió* al text pla.”

- Confusió: Substitució (Cada unitat del missatge substituïda per una unitat de la xifra d'acord amb unes determinades regles).
- Difusió: Transposició (Reordenem les unitats del llenguatge d'acord a un determinat criteri).
- **Entropia** en relació a la informació.
 - Termodinàmica: mesura del desordre.
 - Teoria de la informació: probabilística de trobar un símbol en una posició.

Index

1 Introducció

2 **Criptosistemes clàssics**

- Els inicis i criptografia alquimista
- Xifrat de Vigenère

3 Criptosistemes mecànics

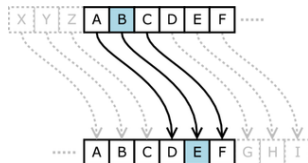
4 Criptosistemes computacionals

Xifrat de Cèsar

- Xifrat monoalfabetic.
- Documentat per l'historiador *Suetonius*.
- Sistema de substitució.
- Formulari:

$$E_n(x) = (x + n) \bmod |\alpha\beta|$$

$$D_n(x) = (x - n) \bmod |\alpha\beta|$$



exemple

- Programari Lliure
- Surjudpdul iilxuh
- Criptoanlisi medieval per freqüències.

Criptografia Alquimista

- Ulls inquisidors: necessitat d'ocultar el significat.
 - Caràcters i símbols estranys.
- Llenguatge erudit i tecnicismes.
 - Conegut per altres estudiosos.
- Recursos:
 - Escriptura sense vocals.
 - Transposició, substitució, esteganografia.
 - Homofonia.
 - Digrafs i trigrafs.

Avenç Renaixentista

- Giovan Batista Belasco:
 - Contrasenyas i frases de pas.
- Gerolamo Cardano (1501 – 1576):
 - Autoclau: elements previs usats per xifrar el següent.
- Giovanni Battista Porta (1538 – 1615):
 - Mescla la disposició dels alfabetos.
- Blaise de Vigenère (1523 – 1596):
 - Compendia tots.

Blaise de Vigenère

Xifrat

- Una lletra clau, xifrar la primera del text pla,
- canvia l'alfabet en base l'anterior lletra clara,
- tenim l'alfabet per a la següent.

Desxifrat

- Desxifrant la primera lletra sabem l'alfabet,
- en desxifrar la lletra, obtenim la clau per a la segona.

Index

- 1 Introducció
- 2 Criptosistemes clàssics
- 3 Criptosistemes mecànics**
 - Mecanització
 - Refinament: Enigma
- 4 Criptosistemes computacionals

Màquines de rotors

- Màquines complexes de *substitució*.
- Automatitzar els processos.
- 26 intercanviadors integrats: *monoalfabetic*.
- Un rotor de 26 intercanviadors: *polialfabetic* (posició inicial).
- Múltiples rotors (N) (iguals símbols i diferent ordre).

$$||\alpha\beta||^N$$

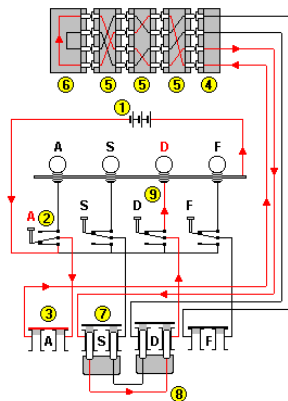
Inventors

- 1795: Thomas Jefferson.
- 1915: Hengel & Spengler, oficina Naval Holandesa.
- 1917: Edward Hugh Herbern, USNavy.
- 1919: Hugo Koch (holanda), Arvid Gerhard Damm (Suïssa).



Enigma

- Inventor: Arthur Scherbius.
- Reflex: una lletra no serà xifra de si mateixa.
- Alta variabilitat:
 - Quins rotors i en quin ordre.
 - Posicions inicials.
 - Posició relativa entre alfabet en el teclat i en la pantalla.
 - Connexions del reflector.



Nota

- Màquina amb moltes variacions i fins a 8 rotors.

Index

- 1 Introducció
- 2 Criptosistemes clàssics
- 3 Criptosistemes mecànics
- 4 Criptosistemes computacionals**
 - Cosos finits
 - Complexitat matemàtica i funcions d'una sola via
 - Corbes El·líptiques

New directions in cryptography

- Diffie, W. y M.E.Hellman. "New directions in cryptography", IEEE Transactions on Information Theory 22 (1976), pp. 644-654.
 - Protocol d'intercanvi de claus simètriques basat en el Problema del Logaritme Discret (DLP):

$$a \equiv b^x \pmod{n}$$

- Ron Rivest, Adi Shamir y Len Adleman del MIT, 1977.
 - Criptosistema basat en el Problema de la Factorització d'Enters (IFP):

$$n = p \cdot q \mid p \neq q$$
$$\phi(n) = (p - 1) \cdot (q - 1)$$

Government Communications Headquarters (GCHQ)

- Fills del 'Bletchley Park'
- Documents desclassificat 1997
 - Clifford Cocks, 1973: Factorització de nombres primers.
 - Malcom Williamsom, 1974: Intercanvi de claus amb logaritme discret.

Funcions d'una sola via

Definició

Un funció $f : X \rightarrow Y$ és una funció d'una sola via si $f(x)$ es:

- *Fàcilment* calculable $\forall x \in X$
- per a *casi* tota $y \in Im(f)$ es difícil trobar un $x \mid f(x) = y$

La funció del Problema del logaritme discret (DLP)

$$\begin{array}{rcl} f : \mathbb{Z}_{>0} & \longrightarrow & G = \langle g \rangle \\ x & \longmapsto & a = g^x \end{array}$$

Orígens el·líptics

- Van ser proposades per a ús criptogràfic (de forma independent):
 - N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203 – 209.
 - V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.
- Però ja formaven part de les matemàtiques des de molt abans
 - Adrien-Marie Legendre (1752 – 1833)
 - Carl Friedrich Gauss (1777 – 1855)
 - Niels Henrik Abel (1802 – 1829)
 - Carl Gustav Jakob Jacobi (1804 – 1851)
 - Joseph Liouville (1809 – 1882)
 - Karl Theodor Wilhelm Weierstraß (1815 – 1897)
 - Bernhard Riemann (1826 – 1866)

Conjunt de punts d'una corba el·líptica

- Equació reduïda de Weierstraß per \mathbb{F}_p (amb $p > 3$):

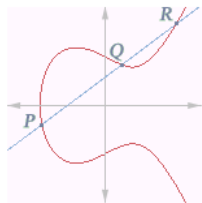
$$y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_p$$

- $E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$
- La funció del Problema del logaritme discret *El·líptic* (ECDLP)

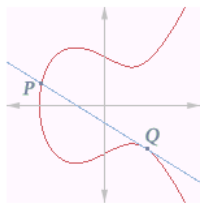
$$\begin{array}{l} \bullet \quad f : E(\mathbb{F}_p) \longrightarrow E(\mathbb{F}_p) = \langle G \rangle \\ \quad \quad P \quad \longmapsto \quad R \quad = x \cdot G \end{array}$$

Conjunt de punts d'una corba el·líptica

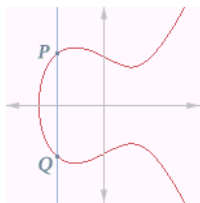
Un exemple gràfic:



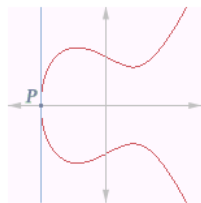
$$P + Q + R = 0$$



$$P + Q + Q = 0$$



$$P + Q + 0 = 0$$



$$P + P + 0 = 0$$

Criptoanàlisi

El millor algorisme *conegut* sobre corbes el·líptiques:

- ρ de Pollard
- sobre $E(\mathbb{F}_p)$ té un cost: $O(\sqrt{n})$, $n = \|E(\mathbb{F}_p)\|$.
- Una màquina amb una capacitat de comput de $10 \cdot 10^9$.
- Sobre $E(\mathbb{F}_{160})$:

cost = $1/2 \cdot 10^{24}$ operacions bàsiques

$$\text{temps} = \frac{\text{cost}}{10 \cdot 10^9 \cdot 60 \cdot 60 \cdot 24 \cdot 365} \approx 38 \cdot 10^6 \text{ anys}$$

On les podem trobar?

Implementacions lliures:

- OpenSSL 0.9.8 (llicència tipus BSD).
- ECCGnuPG 1.4 (llicència GPLv2).
- libgcrypt (**todo**).

Nota: les imatges provenen de *Wikipedia*.