# Breu estudi de la criptografia en les comunicacions mòvils

**Jordi Inglés Camats**

**Francisco Javier Molina Carrillo**

**Maig 2004**

# Índex

# 1. Introducció

- **Criptografia:** *Krypto* (ocult) + *grapho* (escriptura)

  Sistemes criptogràfics de clau privada

  Sistemes criptogràfics de clau pública

- **Comunicacions Wireless**

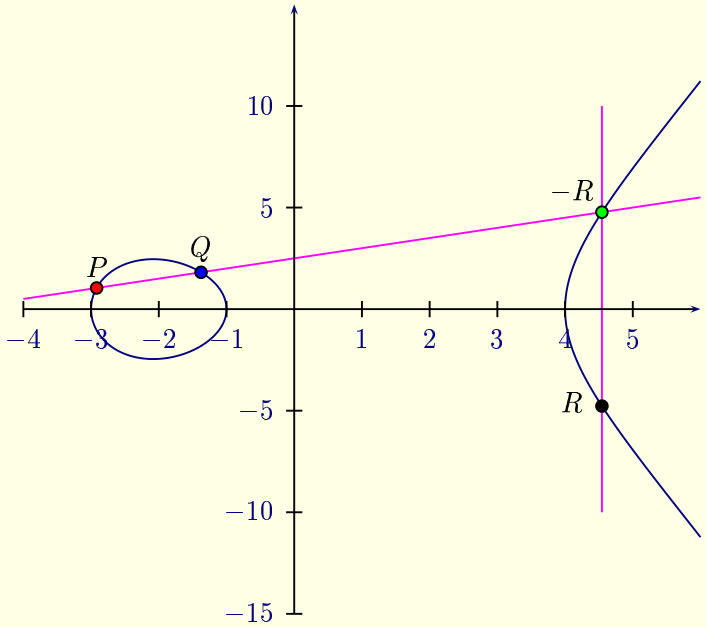
  Capacitat computacional limitada

# 2. Corbes el·líptiques

- **Definició corba el·líptica:**
  Corba cúbica plana no singular

$$E(\mathbb{Z}_p) = \{(x, y) \in \mathbb{Z}_p^2 \mid y^2 = x^3 + ax + b \quad on \quad 4a^3 + 27b^2 \neq 0\} \cup \{O_E\}$$

- **Suma de punts d'una corba el·líptica**



- **Potència d'un punt**

$$n * P = \begin{cases} \underbrace{P + P + \cdots + P}_{n} & \text{si } n > 0 \\ O_E & \text{si } n = 0 \\ \underbrace{(-P) + (-P) + \cdots + (-P)}_{n} & \text{si } n < 0 \end{cases}$$

- **Algorisme del camperol rus**

1. Expressar $n$ en base 2: $n_{10} = (b_i b_{i-1} \ldots b_1 b_0)_2$
2. Substituir cada $b_i = 1$ pel parell e lletres $SX$, i cada $b_i = 0$ per $S$
3. Eliminem al parell $SX$ situat més a l'esquerra
4. Apliquem a $P$ les següents regles de càlcul:

   $S$: multiplcar per 2 i reduïm mòdul $p$

   $X$: sumem $P$ i reduïm mòdul $p$

# 3. El món de la criptografia

## Introducció

- **Objectiu de la criptografia en una transmissió:**
  Garantitzar la privacitat dels missatges, de manera que sols el destinatari del missatge pugui coneixèr-los

- **Definició de protocol criptogràfic:**
  - Conjunt d'etapes
  - Dos o més parts
  - Per a realitxzar una feina específica
  - Algorisme criptogràfic com a eina

- **Tipus de protocols:**
  - Autentificació del missatge
- Autentificació de l'usuari $\begin{cases} directa \\ indirecta \end{cases}$
- **Protocols per Compartir Secrets**
  - $(n, k)-$ esquemes llindar
- **Proves de coneixement zero**
- **Transaccions electróniques segures**
- **Votacions electróniques**

## Criptosistema simètric o de clau compartida

- Emissor i receptor tenen la mateixa clau privada
- 5-tupla $(\mathcal{M},\mathcal{C},\mathcal{K},c,d)$, on:

  $\mathcal{M}$: conjunt de missatges originals (o missatges en clar)

  $\mathcal{C}$: conjunt de missatges xifrats

  $\mathcal{K}$: conjunt finit de claus

  i les funcions:

  $c$: $\mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C}$, donat un missatge $M \in \mathcal{M}$ i una clau $K \in \mathcal{K}$ s'obté el missatge xifrat $C \in \mathcal{C}$

  $d$: $\mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M}$, donat un missatge xifrat $C \in \mathcal{C}$ i una clau $K \in \mathcal{K}$ s'obté el missatge en clar $M \in \mathcal{M}$

- **Desavantatges**
  - Distribució de claus
  - Emmagatzemament de claus
  - Actualització de claus
  - No possibilitat de firma digital

## Criptosistema asimètric o de clau pública

- Utilitzem doble clau $(K_p, K_u)$
- 6-tupla ($\mathcal{M}$,$\mathcal{C}$,$\mathcal{K}$,$c$,$d$), on:

  $\mathcal{M}$: conjunt de missatges originals (o missatges en clar)

  $\mathcal{C}$: conjunt de missatges xifrats

  $\mathcal{K}$: conjunt finit de claus

  i les funcions:

  $c$: $\mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C}$, donat un missatge $M \in \mathcal{M}$ i una clau $K \in \mathcal{K}$ s'obté el missatge xifrat $C \in \mathcal{C}$

  $d$: $\mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M}$, donat un missatge xifrat $C \in \mathcal{C}$ i una clau $K \in \mathcal{K}$ s'obté el missatge en clar $M \in \mathcal{M}$

- **Característiques:**
  - Resolen els problemes de distribució de claus i autentificació
  - El coneixement de $K_u$ no permet calcular $K_p$
  - Es poden utilitzar per establir connexions segures per canals insegurs
  - Possibilitat d'aplicar firma digital
  - Computacionalment més costosos i xifras més lent

## Criptosistema DES

- DES (Data Encription Standard)
- Realitzat per IBM i publicat com a estàndard el 1977
- Criptosistema de bloc i de clau compartida que xifra i desxifra blocs de 64 bits emprant una clau de 56 bits

## La funcio hash SHA

- **Definició de funció hash:**
  Funció matemàtica que realitza un resum del document a signar

- Funció irreversible

- Algorisme del SHA (Secure Hash Algorithm) desenvolupat per NSA

- Produir reums de 160 bits a partir de blocs de 512 bits del missatge original

## Criptosistema ElGamal

- **Definicions prèvies**
  Sigui $G$ un grup i $a \in G$:
  - **Ordre de $G$:**
    Nombre d'elements que té el grup $G$. Si l'ordre de $G$ és finit direm que $G$ és un **grup finit**
  - **Subgrup generat per $a$:**
    $< a >= a' : i \geq 0$
  - **Element primitiu o generador de $G$:** $< a >= G$, on $G$ serà un **grup cíclic**

- **Problema del logaritme dicret:**
  Donat un grup cíclic $G$ d'ordre $n$, un generador $g \in G$ i un element $b \in G$, trobar un enter $x$, $0 \leq x < n$ tal que $g^x = b$, i per tant $x = \log_g b$

- **Problema de Diffie-Hellman:**
  Donat un grup finit cíclic $G$, un generador $g \in G$ i donat un parell d'elements $g^a$ i $g^b$, trobar $g^{ab}$

- **Logaritme discret el·líptic**
  - La dificultat per resoldre el problema del logaritme discret pot variar segons el grup en que es treballi
  - Avantatges ús corbes el·líptiques:
    - Atacs al problema del logaritme discret més difícils
    - Ús de grups de mida menor. Els còmputs necessaris més simples
    - Fixat un cos $\mathbb{Z}_p$, existeixen moltes corbes el·líptiques sobre aquest

# ElGamal

- **Procés per generar les claus:**
  1. Escollir un grup cíclic $G$ d'ordre $n$ i un generador $g$
  2. Seleccionem un enter $x$, $1 \leq x \leq n-1$ i calculem $g^x$
  3. $k_u = (g, g^x)$ i $k_p = x$
- **Xifrat de missatges:**
  $B$ vol enviar un missatge $M$ a $A$
  1. Obtenim la clau pública de $A$ $k_{uA} = (g, g^{x_A})$
  2. Seleccionar aleatoriament $k$ tal que $1 \leq k \leq n-1$
  3. Calculem $y = g^k$ i $r = M \cdot (g^{x_A})^k$
  4. Enviar el missatge xifrat $c = (y, r) = \left(g^k, M \cdot (g^{x_A})^k\right)$ a $A$
- **Desxifrat de missatges:**
  $A$ reb el missatge $c$ de $B$
  1. $A$ utilitza $k_p A = x_A$ per calcular:
     $t = y^{x_A} = \left(g^k\right)^{x_A}$, i a partir d'aquest calcular $t^{-1}$
  2. $r \cdot t^{-1} = M \cdot (g^{x_A})^k \cdot t^{-1} = M \cdot (g^{x_A})^k \cdot \left(\left(g^k\right)^{x_A}\right)^{-1} = M$

## Firma digital amb ElGamal

$A$ signa el missatge $M$

1. Escollir un nombre aleatori $k$, $2 \leq k \leq n-2$, tal que $mcd\,(k, n) = 1$
2. Calcular $r = g^k$
3. Calcular $k^{-1}$ mod $n$
4. Calcular el hash de $M$, $H\,(M)$
5. Calcular $s = k^{-1}\,(H\,(M) + x_A \cdot r)$ mod $n$
6. La signatura de $A$ del missatge $M$ serà $(r, s)$

$B$ verifica la signatura de $A$

1. Obtenir $k_{uA} = (g, g^{x_A})$
2. Calcular $H\,(M)$
3. Calcular $v_1 = ((g^{x_A})^r) - 1 \cdot r^s$
4. Calcular $v_2 = g^{H(M)}$
5. Acceptar la signatura si $v_1 = v_2$

# 4. El protocol wireless

Paràmetres en comú: corba el·líptica $E$, punt $P \in E$ d'ordre $n$ gran

- **Generació de claus**

  Escollir un enter a l'atzar $d \in [2, n-2]$.

  $Q = dP$.

  Clau pública de A: $(E, P, n, Q)$ Clau privada de A: $d$.

- **Firma de la clau per l'autoritat certificadora**

| USUARI | | AUTORITAT CERTIFICADORA |
|---|---|---|
| Escollir $d \in [2, n-2]$ | | Escollir $k \in [2, n-2]$ |
| $Q = dP$ | | $R = kP$ |
| Envia | $\xrightarrow{Q}$ | Rebre |
| | | Escollir un unic $I$ |
| | | $r = R.x$ |
| | | $s = k^{-1}\left(H\left(Q.x, I, t\right) + d_{ca} \cdot r\right)$ |
| Rebre | $\xleftarrow{Q_{ca}, I, (r,s), t}$ | Envia |
| $e = H\left(Q.x, I, t\right)$ | | |
| Emmagatzema | | |
| $Q, Q_{ca}, I, (r, s), e, t$ | | |

# Autentificació entre client i servidor

| CLIENT | | SERVIDOR |
|---|---|---|
| Rebre | $\xleftarrow{Q_s}$ | Enviar |
| Generar un nombre a l'atzar $g_u$ | | |
| Enviar | $\xrightarrow{Q_u, g_u}$ | Rebre |
| $Q_k = d_u Q_s = (d_u \cdot d_s) P$ | | $Q_k = d_s Q_u = (d_s \cdot d_u) P$ |
| La clau mútua acordada és $Q_k.x$ | | La clau mútua acordada és $Q_k.x$ |
| | | Generar un nombre aleatori $g_s$ |
| | | $C_0 = E(Q_k.x, (e_s, (r_s, s_s), t_s, g_u, g_s))$ |
| Rebre | $\xleftarrow{C_0}$ | Enviar |
| $D(Q_k.x, C_0)$.Mirar si és present $g_u$ | | |
| $C_1 = E(Q_k.x, (e_u, (r_u, s_u), t_u, g_s))$ | | |
| Enviar | $\xrightarrow{C_1}$ | Rebre |
| | | $D(Q_k.x, C_1)$ |

| CLIENT | SERVIDOR |
| --- | --- |
| | Si $g_s$ i $t_u$ són válids |
| $c = s_s^{-1}$ | $c = s_u^{-1}$ |
| $u1 = c \cdot e_s$ | $u1 = c \cdot e_u$ |
| $u2 = c \cdot r_s$ | $u2 = c \cdot r_u$ |
| $R = u1P + u2Q_{ca}$ | $R = u1P + u2Q_{ca}$ |
| $v = R.x$ | $v = R.x$ |
| Si $v \neq r_s$, llavors abortar | Si $v \neq r_u$, llavors abortar |
| $k_m = H\left(Q_k.x, g_s, g_u\right)_{msb64}$ | $k_m = H\left(Q_k.x, g_s, g_u\right)_{msb64}$ |
| $k_m$ és la clau secreta que s'utilitzarà | $k_m$ és la clau secreta que s'utilitzarà |

# 5. Bibliografia


- W. Diffie and M. E. Hellman. *New directions in cryptography. IEE Trans. Inform. Theory*

- M.Aydos, T. Tanik, Ç.K.Koç. *High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor*. Electrical  Computer Engineering Oregon State University

- M. José Lucena López. *Criptografia y Seguridad en Computadores*. Departamento de Informática. Escuela Politécnica Superior. Universidad de Jaén

- **www.google.es!!!!**