College Cryptografie

Cursusjaar 2007

Openbare sleutelsystemen

28 januari 2007

Principe

Getaltheorie

Diffie-Hellman (1976)

RSA (1978)

ElGamal (1984)

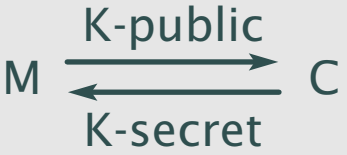
Merkle-Hellman (1978)

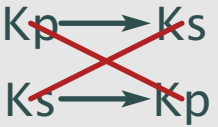
Priemgetallen

Elliptische krommen

Klassieke versus Publickey cryptografie

klassiek





publickey

Functies te vinden waarmee:

- encryptie *eenvoudig*
- ongewenste decryptie *ondoenlijk*
- afleiden geheime uit openbare sleutel *ondoenlijk*

one way functie

eenvoudig: $y = f(x)$ onuitvoerbaar: $x = f^{-1}(y)$

trapdoor one way functie

onuitvoerbaar: $x = f^{-1}(y)$ eenvoudig: $x = f^{-1}(y, z)$

algoritmische complexiteit

- eenvoudig = $\mathcal{O}(n^c)$ *polynomiaal*
- ondoenlijk = $\mathcal{O}(c^n)$ *exponentieel*
- zoeken n-bit sleutel = $\mathcal{O}(2^n)$

functiebron getaltheorie

- discrete logaritme
- factorisatie

Functietype

$$x \in \mathbb{Z} \rightarrow (x \bmod n) \in \mathbb{Z}_n$$

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, \ldots, 8, 9\}$$

$$\mathrm{Z}_n^* = \{x \in \mathbb{Z}_n : x > 0 \wedge \mathrm{ggd}(x, n) = 1\}$$

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

primitief element $x^0, x^1, x^2, \ldots = \mathbb{Z}_n^*$

$$(3, 7) \rightarrow \mathbb{Z}_{10}^* \; (1, 9) \not\rightarrow \mathbb{Z}_{10}^*$$

Voor $\mathbb{Z}_n^*$ geldt:

1. $\forall x, y: a * x \equiv a * y \bmod n$ iff $x \equiv y \bmod n$
2. $a * \mathbb{Z}_n^* = \{a * x \bmod n : x \in \mathbb{Z}_n^*\} = \mathbb{Z}_n^*$
3. $\exists b \in \mathbb{Z}_n^* : a * b \equiv 1 \bmod n$

Daarmee $\mathbb{Z}_n^*$ abelse groep onder vermenigvuldiging $\bmod n$

p priem $\rightarrow \mathbb{Z}_p^* + \{0\} = \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is *eindig veld* $GF(p)$

Stelling van Euler

$$\text{ggd}(p, n) = 1 \rightarrow p^{\phi(n)} \equiv 1 \bmod n$$

Euler totient functie

$$\phi(n) = \#i \text{ met } \text{ggd}(i, n) = 1 \text{ voor } i = 1, 2, \ldots, n-1$$

$$\phi(p) = (p-1) \text{ voor } p \text{ priem}$$

$$\phi(p \cdot q) = (p-1)(q-1) \text{ voor } p, q \text{ priem}$$

Kwadratische rest $x \bmod p$ *als*

$$\exists y \in \mathbb{Z}_p^*\colon y^2 \equiv x \bmod p \rightarrow x \in \mathbb{Q}_p$$

Legendre symbool

$$L(a,p) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ +1 & \text{if } a \in \mathbb{Q}_p \\ -1 & \text{if } a \notin \mathbb{Q}_p \end{cases}$$

Jacobi symbool

$$J(a,n) = \left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^{e_1}\left(\frac{a}{n}\right)^{e_2} \ldots \quad n = p_1^{e_1} p_2^{e_2} \ldots$$

parameters

- *openbare* informatie
  $GF(q)$ met q priem
  primitief element $a \in GF(q)$
- *geheime* informatie
  deelnemer i getal $x_i \in GF(q)$
- *openbare* informatie
  deelnemer publiceert
  $y_i = a^{x_i} \bmod q$
- sleuteluitwisseling

uitvoering

- i = *verzender* sleutel

$$K_{ij} = a^{x_i x_j} = (a^{x_j})^{x_i} = y_j^{x_i}$$

- j = *ontvanger* sleutel

$$K_{ij} = a^{x_i x_j} = (a^{x_i})^{x_j} = y_i^{x_j}$$

veiligheid

- $y_i = a^{x_i} \bmod q$ eenvoudig
- $x_i = \log_a y_i \bmod q$ moeilijk

parameters

- *geheime* informatie
  twee priemgetallen p en q
- *geheime* sleutel
  d met $\text{ggd}(d, \phi(n)) = 1$
- *openbare* informatie
  product $n = p \cdot q$
- *openbare* sleutel
  e met $ed \equiv 1 \bmod \phi(n)$
- authenticatie kan omdat

$$M = D(E(M)) = E(D(M))$$

uitvoering

- *verzender* bericht

$$C = E(M) = M^e \bmod n$$

- *ontvanger* bericht

$$M = D(C) = C^d \bmod n$$

veiligheid

- p, q groot, $n \approx 300$ cijfers
- p en q uit n: $\mathcal{O}\left(e^{\sqrt{\log n \log\log n}}\right)$
- zorgvuldig kiezen p, q, d, e

RSA acroniem voor R = Rivest, S = Shamir, A = Adleman

RSA (1978)

$$D(E(M)) = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n$$

$$ed \equiv 1 \bmod \phi(n) \rightarrow ed = k.\phi(n) + 1$$

$$\begin{aligned} M^{ed} \bmod n &= M^{k.\phi(n)+1} \bmod n \\ &= M.M^{k.\phi(n)} \bmod n \\ &= M.(M^{\phi(n)} \bmod n)^k \bmod n \end{aligned}$$

$$M^{\phi(n)} \equiv 1 \bmod n \text{ (Euler)} \rightarrow (M^{\phi(n)} \bmod n)^k = 1^k \bmod n = 1$$

$$M^{ed} \bmod m = M.1 \bmod n = M$$

- kies RSA parameters:
  1. $(p, q) = (47, 59) \rightarrow n = 2773$
  2. $\phi(n) = 46.58 = 2668$
  3. kies $d = 157$
  4. $\mathrm{ggd}(2668, 157)$ berekening $\rightarrow$

     $e = 17$ en $e \cdot d = 17.157 \equiv 1 \bmod 2668$
- codeerschema: spatie (–) = 00, A = 01, B = 02, . . . , Z = 26
- vercijfering:

	I T	**S -**	**A L**	**L -**	**G R**	**E E**	**K -**	**T O**	**- M**	**E -**
M:	**0920**	**1900**	**0112**	**1200**	**0718**	**0505**	**1100**	**2015**	**0013**	**0500**
C:	**0948**	**2342**	**1084**	**1444**	**2663**	**2390**	**0778**	**0774**	**0219**	**1655**

$0920^{17} = 0920^{10001_2} = 0948 \longleftrightarrow 0948^{157} = 0920$

Voorbeeld RSA vercijfering

- factorisatie forecast uit 1985

cijfers	bits	schatting	realisatie
100	332	1 jaar	1994: RSA-129
125	415	100 jaar	1996: RSA-130
150	498	10.000 jaar	1999: RSA-140
175	581	700.000 jaar	1999: RSA-155
200	664	30 miljoen jaar	2005: RSA-200
225	747	1 miljard jaar	
308	1024	nagenoeg ∞	

- RSA Laboratories challenges, bv. 193 cijfers $ 20.000.
- algoritmen voor factorisatie 'hot research topic'

- FOUT gemeenschappelijke priemfactor $n_i = p \cdot q_i$
- FOUT meerdere e, d bij een enkele $n = p \cdot q$
- identieke berichten, verschillende n maar dezelfde e
  soms $\mathbb{Z}_n \to \mathbb{Z}$ reductie mogelijk
- lage openbare exponent e en deels bekende klaartekst
  bijvoorbeeld padding 64 bit sleutel naar 1024 bit blok
- lage geheime exponent d gekoppeld met $|p - q|$
  kettingbreukontwikkeling van e/n kan d opleveren

Zwakke plekken in RSA

parameters

- *geheime* informatie
  encryptie exponent s
- *openbare* informatie
  p priem $\mathbb{Z}_p$, $a \in \mathbb{Z}_p$
  getal $b = a^s \bmod p$
- *geheime* sleutel $k \in \mathbb{Z}_{p-1}$

veiligheid

- discrete logaritme
  $s = \log_a b \bmod p$
  ondoenlijk

uitvoering

- *verzender* bericht
  $C = (c_1, c_2) = (M.b^k,\ a^k)$
- *ontvanger* bericht
  $M = D(c_1, c_2) = c_1 c_2^{-s}$
  $= (M.b^k)(a^k)^{-s}$
  $= M.b^k.(a^s)^{-k}$
  $= M.b^k b^{-k} \bmod p = M$
- valkuil
  $C = E(M,k), C' = E(M',k)$
  $M.c_1^{-1}c_1' =$
  $M.(M^{-1}b^{-k})(M'b^k)$
  $M.M^{-1}.M' = M'$

ElGamal (1984)

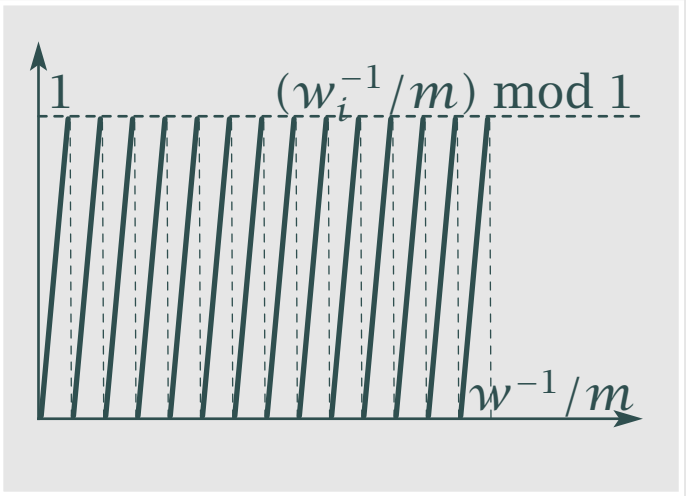
parameters

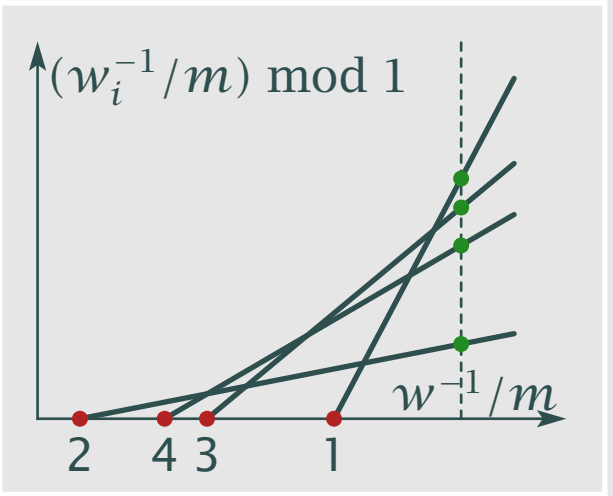
- *geheime* informatie
  knapzakvector is
  $$\vec{a} = (a_1, a_2, \ldots, a_n)$$
  superstijgend $a_i > \sum_{j=1}^{i-1} a_j$
  $w, m > \sum_{i=1}^{n} a_i$
  $\text{ggd}(w, m) = 1$
- *openbare* informatie
  $\vec{b} = (b_1, b_2 \ldots, b_n)$
  $b_i = w.a_i \bmod m$, $\pi(\vec{b})$
- *veiligheid* op drijfzand
  superstijgend < NP-compleet

uitvoering

- *verzender* bericht
  $M = \vec{x} = (x_1, x_2, \ldots, x_n)$
  $C = \vec{b}.\vec{x} = \sum_{i=1}^{n} b_i x_i$
- *ontvanger* bericht
  $w^{-1}C = w^{-1}\vec{b} \cdot \vec{x}$
  $= w^{-1} \sum_{i=1}^{n} b_i x_i \bmod m$
  $= \sum_{i=1}^{n} w^{-1}w.a_i x_i \bmod m$
  $= \sum a_i x_i \bmod m = \vec{a} \cdot \vec{x}$
  superstijgende $\vec{a}$ splitst $\vec{a} \cdot \vec{x}$
  en dan $\pi^{-1}(\vec{a}) \rightarrow M$

Merkle-Hellman (1978)





- reduceer $\forall b_i \approx 2^{200}$ met w^{-1}/m tot $a_1 \approx 2^{100} \ldots a_{100} \approx 2^{200}$
- kans cluster $P(i) \approx 2^{3n-ni+i(i-1)/2}$: $i = 4, n = 100, P \approx 2^{-94}$
- polynomiaal algoritme L3 (Lenstra, Lenstra en Lovacz)

Shamir breekt knapzak (1982)

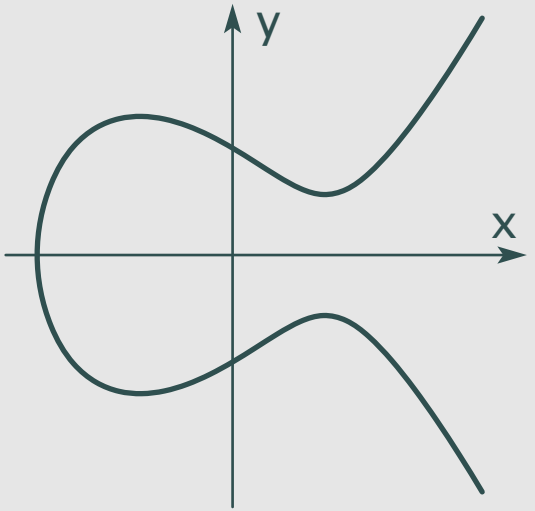
- aantal priemgetallen in $[2 \ldots x]$ is $\pi(x) \approx \frac{x}{\ln x}$ (Gauss)
- $N(100) = \pi(10^{100}) - \pi(10^{99}) \approx 4.10^{97}$
- gemiddeld $\delta(p_i \to p_{i+1}) \approx \ln x$ bij 150 cijfers $\delta \pm 345$
- *sterke* priemgetallen (systematisch te vinden)

  1. $p - 1$ grote priemfactor q
  2. $p + 1$ grote priemfactor r
  3. $q - 1$ grote priemfactor

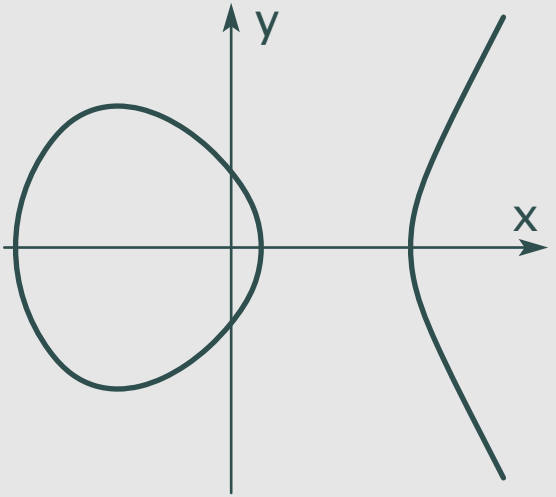
- state of the art 1024 bit RSA: p, q elk ongeveer 150 cijfers

- deterministisch
  speciale gevallen zoals *Mersenne* priemgetallen
- probabilistisch
  - Solovay-Strassen
    Euler getuige a voor n **niet priem**:
    $\gcd(a,n) > 1$ én/of $J(a,n) \not\equiv a^{(n-1)/2} \bmod n$
    Euler leugenaar a voor n **niet priem maar toch**:
    $\gcd(a,n) = 1$ én $J(a,n) \equiv a^{(n-1)/2} \bmod n$
    leugenaar heeft 50%, na k onafhankelijke testen 2^{-k}
  - Miller-Rabin
    sterke getuige of *sterke leugenaar* a hier 25% kans

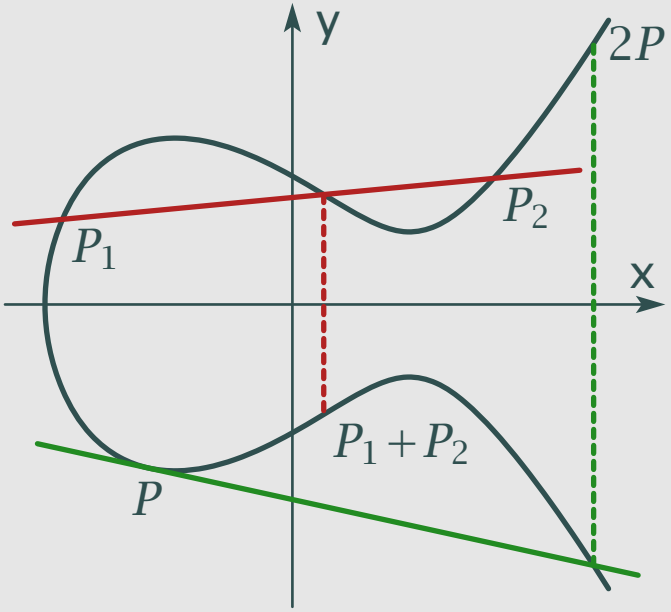
$$y^2 = x^3 + ax + b$$



1-delige kromme



2-delige kromme



$$y^2 = x^3 + ax + b$$

$$P_s = \begin{cases} x_s = \lambda^2 - x_1 - x_2 \\ y_s = \lambda(x_1 - x_s) - y_1 \end{cases}$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{als } P_1 \neq P_2 \\ \\ \frac{3x_1^2 + a}{2y_1} & \text{als } P_1 = P_2 \end{cases}$$

Elementen $GF(p)$ of $GF(2^n)$ afbeelden met $y^2 = x^3 + ax + b$

Sommeren van punten