Hoe je het cryptosysteem RSA *soms* kunt kraken

Benne de Weger

TU/e
Technische Universiteit
Eindhoven
University of Technology

28 aug. / 4 sept. 2010

RSA

asymmetrisch cryptosysteem

versleutelen met de publieke sleutel

ontsleutelen met de bijbehorende privé-sleutel

gebaseerd op getaltheorie / modulo-rekenen

veiligheid gebaseerd op moeilijk zijn van ontbinden in priemfactoren ...

... maar daar is wel meer over te zeggen

modulo-rekenen

vast getal m als *modulus*

delen met rest, behoud alléén de rest

notatie: $a \equiv b \pmod{m}$ betekent:
$a - b$ is een m-voud

reduceren $\pmod{m}$:
terugbrengen tot $\{0, 1, 2, \ldots, m-1\}$

$m = 12$ (of 24): klokrekenen

RSA: een sleutelpaar

twee priemgetallen p en q

hun product $n = p \cdot q$ is de modulus

$\varphi(n) = (p-1) \cdot (q-1)$ (functie van Euler)

kies willekeurige e (*publieke exponent*)

e, n vormen de *publieke sleutel*

bereken d (*privé-exponent*) zodat

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

d, n vormen de *privé-sleutel*

RSA: versleutelen en ontsleutelen

geheim coderen als getal m (*klare tekst*)

m versleutelen tot c (*geheimschrift, cijfertekst*)
met de publieke sleutel:

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

c ontsleutelen met de privé-sleutel:

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

moet weer de klare tekst m opleveren

RSA: verklaring

Stelling van Euler: $a^{\varphi(n)} \equiv 1 \pmod{n}$
(mits ggd$(a, n) = 1$)

ontsleutelde cijfertekst

$$\equiv c^d \equiv (m^e)^d = m^{e \cdot d}$$

$$= m^{1+k \cdot \varphi(n)} = m \cdot \left(m^{\varphi(n)}\right)^k$$

$$\equiv m \cdot 1^k = m \pmod{n}$$

$=$ originele klare tekst

RSA: kraken

tegenstander heeft alleen publieke informatie

publieke sleutel: e en n

cijfertekst: c

zij wil geheime informatie achterhalen

liefst de privé-exponent d

dat kan door n in zijn factoren p, q te ontbinden

dan zijn $\varphi(n)$ en d te berekenen

factoriseren is moeilijk

NH 12-01-10 katern 1 pagina 08

Digitale beveiliging weer wat minder veilig

Wiskundigen ontbinden een getal van 232 cijfers in twee priemgetallen en vestigen een record

Een nieuw wereldrecord in het ontbinden van een groot getal in twee priemgetallen betekent dat de beveiligers van digitale informatie naar nóg grotere getallen moeten uitwijken.

Door BENNIE MOLS

ROTTERDAM, 12 JAN. Een groep wiskundigen is erin geslaagd een getal van 232 cijfers te ontbinden in zijn twee priemdelers, priemgetallen met elk 116 cijfers. Daarmee hebben zij een nieuw wereldrecord gevestigd. Deze wereldrecords – het vorige is van vijf jaar geleden met een getal van 200 cijfers – zijn belangrijk, omdat de beveiliging van bijvoorbeeld het elektronische betalingsverkeer gebaseerd is op cryptografische versleutelingen met zulke grote getallen die in twee priemgetallen te ontbinden zijn.

De internationale groep, waaronder wiskundigen van het Centrum Wiskunde en Informatica in Amsterdam (CWI), heeft een wetenschappelijke publicatie over de priemgetallenontbinding aangeboden aan het elektronische preprintarchief *Cryptology*.

Priemgetallen zijn getallen die alleen deelbaar zijn door 1 en zichzelf. Ze spelen een cruciale rol in de beveiliging van digitale informatie. Wie via een beveiligde website zijn bankzaken doet of een bestelling betaalt, maakt er automatisch gebruik van. Die beveiliging, de zogeheten RSA-cryptografie (vernoemd naar de bedenkers Rivest, Shamir en Adleman) gebruikt grote gehele getallen die het product zijn van twee priemgetallen.

Het getal 15 is een voorbeeld van een getal waarvan we snel zien dat het ontbonden kan worden in twee priemgetallen, want: 3 × 5 = 15. Hoe groter het getal, hoe moeilijker het wordt om te weten of een getal een product is van twee priemgetallen én om die twee 'priemdelers' te vinden. Niemand heeft nog een oplossing gevonden voor dit 'factorisatieprobleem'.

> Het kraken van creditkaartcodes kost nog duizend keer zo veel rekentijd

De onwaarschijnlijkheid om getallen van een paar honderd cijfers snel te ontbinden in twee grote priemdelers ligt aan de basis van RSA-cryptografie. De beveiligers nemen twee grote priemgetallen en vermenigvuldigen die met elkaar. Het grote getal is daarna de beveiligingssleutel die de boodschap codeert. Een kwaadwillende kan de code alleen kraken als hij beide grote priemdelers kent. En dat kan alleen door het grote getal te ontleden in de priemgetallen – met brute rekenkracht.

Om de betrouwbaarheid van digitale beveiligingen te testen en nieuwe standaarden te bepalen, proberen wiskundigen met razendsnelle computers steeds grotere getallen te ontbinden in priemdelers. In feite vermenigvuldigen ze steeds twee grote priemgetallen, tot ze hebben bevestigd of uitgesloten dat een bepaald getal een product is van twee priemgetallen. Voor het nieuwe wereldrecord zou een gewone personal computer 1.700 jaar moeten rekenen. Door het kraken te verdelen over honderden snelle computers gaf 'RSA-768' (de 232 decimale cijfers van het getal zijn digitaal weergegeven in 768 bits) in 2,5 jaar zijn twee priemdelers prijs.

Die gekraakte 768-bits-sleutel wordt vrijwel alleen nog gebruikt voor het versleutelen van niet al te gevoelige informatie, die maar een paar weken geheim hoeft te blijven. Voor kwaadwillenden is het nog steeds geen peulenschil om zulke informatie te ontcijferen. Zij moeten over minstens dezelfde rekenkracht beschikken als de wiskundigen hebben gebruikt.

Gevoelige informatie die lange tijd geheim moet blijven, bijvoorbeeld een creditcardcode, wordt beveiligd met sleutels van 1.024 bits (309 decimale cijfers). Die zijn nog niet gekraakt en voorlopig veilig. „Het kraken daarvan is nog duizendmaal rekenintensiever", zegt Herman te Riele van het CWI, die aan het kraken van RSA-768 meewerkte. „Tien jaar geleden lag het wereldrecord bij een sleutel van 512 bits en vijf jaar geleden bij 663 bits. Ruwweg heb je voor iedere 256 bits extra duizendmaal zo veel rekentijd nodig om de priemdelers te vinden. We verwachten dat we over tien jaar een sleutel van 1.024 bits kunnen kraken. Eigenlijk zou je sleutels van 768 bits al niet meer moeten gebruiken. En over tien jaar zou een sleutel van ten minste 1.280 bits standaard moeten zijn."

maar soms niet...

er zijn 'zwakke sleutels'
en soms heb je een hint

de methode van Mike Wiener

veronderstel $d < \sqrt[4]{n}$ (dan zal $e \approx n$)

er is een k zodat $\boxed{e \cdot d = 1 + k \cdot \varphi(n)}$

omdat $\varphi(n) = (p-1) \cdot (q-1) \approx p \cdot q = n$

volgt $k < d < \sqrt[4]{n}$

n en $\varphi(n)$ liggen dicht bij elkaar:

$n - \varphi(n) = p + q - 1 \approx 2\sqrt{n}$

onbekende $\varphi(n)$ vervangen door bekende n

geeft maar een kleine fout

bekend getal benaderen met breuk

$e \cdot d = 1 + k \cdot \varphi(n) \approx 1 + k \cdot n$ geeft

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \frac{|e \cdot d - k \cdot n|}{n \cdot d} \approx \frac{k \cdot |\varphi(n) - n|}{n \cdot d}$$

$$\approx \frac{2k \cdot \sqrt{n}}{n \cdot d} \approx \frac{1}{\sqrt{n}}$$

hoe vind je een onbekende breuk $\frac{k}{d}$,

met teller en noemer $< \sqrt[4]{n}$,

dicht bij het bekende getal $\frac{e}{n}$?

kettingbreuk, 1e voorbeeld

$\frac{23}{16} = 1 + \frac{7}{16}$,

$\frac{16}{7} = 2 + \frac{2}{7}$ dus $\frac{23}{16} = 1 + \frac{1}{2+\frac{2}{7}}$,

$\frac{7}{2} = 3 + \frac{1}{2}$ dus $\frac{23}{16} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{2}}}$,

$\frac{2}{1} = 2 + \frac{0}{2}$, proces stopt

notatie: $\frac{23}{16} = 1 + \frac{1}{2+\frac{1}{3+\frac{1}{2}}} = [1, 2, 3, 2]$

benaderingen, 1e voorbeeld

$$\frac{23}{16} = [1, 2, 3, 2]$$

$$[1] = 1, \text{ en } \left|\frac{23}{16} - 1\right| = 0.4375$$

$$[1, 2] = \frac{3}{2}, \text{ en } \left|\frac{23}{16} - \frac{3}{2}\right| = 0.0675$$

$$[1, 2, 3] = \frac{10}{7}, \text{ en } \left|\frac{23}{16} - \frac{10}{7}\right| = 0.00625$$

$$[1, 2, 3, 2] = \frac{23}{16}, \text{ en } \left|\frac{23}{16} - \frac{23}{16}\right| = 0$$

kettingbreuk, 2e voorbeeld

$\pi = 3 + 0.14159\ldots,$

$1/0.14159\ldots = 7.06251\ldots,$

$1/0.06251\ldots = 15.99659\ldots,$

$1/0.99659\ldots = 1.00341\ldots,$

$1/0.00341\ldots = 292.63459\ldots,$ dus

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \ldots}}}} = [3, 7, 15, 1, 292, \ldots]$$

benaderingen, 2e voorbeeld

$$\pi = [3, 7, 15, 1, 292, \ldots]$$

$$[3] = 3, \text{ en } |\pi - 3| = 0.14159\ldots$$

$$[3, 7] = \tfrac{22}{7}, \text{ en } \left|\pi - \tfrac{22}{7}\right| = 0.00126\ldots$$

$$[3, 7, 15] = \tfrac{333}{106}, \text{ en } \left|\pi - \tfrac{333}{106}\right| = 0.000083\ldots$$

$$[3, 7, 15, 1] = \tfrac{355}{113},$$
$$\text{en } \left|\pi - \tfrac{355}{113}\right| = 0.00000026\ldots$$

beste benaderingen

Definitie: $\frac{T}{N}$ heet *beste benadering* van α als iedere breuk die dichter bij α ligt, grotere teller en noemer heeft

Stelling: Als α de kettingbreuk $\alpha = [a_0, a_1, a_2, \ldots]$ heeft, dan zijn de *convergenten* $[a_0]$, $[a_0, a_1]$, $[a_0, a_1, a_2,]$, $[a_0, a_1, a_2, a_3]$, $\ldots$ precies de beste benaderingen van α

ongelijkheden voor convergenten

Stelling: Als α de kettingbreuk $\alpha = [a_0, a_1, a_2, \ldots]$ heeft, met convergenten $\dfrac{T_i}{N_i} = [a_0, a_1, a_2, \ldots, a_i]$, dan

$$\frac{1}{(a_{i+1}+2)\cdot N_i^2} < \left|\alpha - \frac{T_i}{N_i}\right| < \frac{1}{a_{i+1}\cdot N_i^2}$$

Voorbeeld: $\left|\pi - \frac{355}{113}\right| = \frac{1}{293.57\ldots\cdot 113^2}$

voldoende voorwaarde

Stelling: Als $\frac{T}{N}$ voldoet aan $\left|\alpha - \frac{T}{N}\right| < \frac{1}{2N^2}$

dan is het een convergent van α

en kun je $\frac{T}{N}$ dus vinden in de kettingbreuk

toepassing

we hadden $\left|\frac{e}{n} - \frac{k}{d}\right| \approx \frac{1}{\sqrt{n}}$ en $d < \sqrt[4]{n}$,

dus met een beetje geluk $\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$

dus de onbekende $\frac{k}{d}$ is een convergent

uit de kettingbreuk van de bekende $\frac{e}{n}$

(als $d \ll \sqrt[4]{n}$: vlak voor een groot wijzergetal)

en nu nog factoriseren

als je d en k weet, dan weet je

$$\varphi(n) = \frac{e \cdot d - 1}{k}$$

en dus weet je $p + q = n + 1 - \varphi(n)$

we wisten al $p \cdot q = n$

dus zijn p en q te vinden met de abc-formule

voorlopige conclusie

een kleine privé-exponent d lekt informatie
via de combinatie van e en n

met leuke getaltheorie is RSA dan te kraken

werkt voor $d < \sqrt[4]{n}$

kun je meer met geavanceerdere getaltheorie?

de methode van Boneh en Durfee

de RSA-vergelijking:

$$e \cdot d = 1 + k \cdot (n + 1 - (p + q))$$

modulo e bekijken: je bent de onbekende d kwijt!

polynoom $f(x, y) = x \cdot y - (n + 1) \cdot x - 1$
heeft nulpunt $(x, y) = (k, p + q)$ modulo e

als d klein is, dan is dit nulpunt klein
t.o.v. de modulus e,
want $k < d$ en $p + q \approx 2\sqrt{n}$ en $e \approx n$

ideeën van Don Coppersmith

1: als een polynoom $g(x, y)$ een klein nulpunt $(x_0, y_0) \pmod M$ heeft
en ook de coëfficiënten van g zijn klein t.o.v. de modulus M,
dan moet wel $g(x_0, y_0) = 0$

2: uit een $f(x, y)$ met grote coëfficïenten kun je polynomen $g(x, y)$ maken
met kleinere coëfficïenten
en met hetzelfde nulpunt $\pmod M$

stelling van Howgrave-Graham

Stelling: Als $h(x, y)$ een polynoom
met ≤ 4 termen
en een nulpunt $(x_0, y_0) \pmod{M}$
met $|x_0| \leq X, |y_0| \leq Y$
en alle coëfficiënten van $h(x \cdot X, y \cdot Y)$ zijn
in absolute waarde $< \frac{1}{2}M$,
dan is $h(x_0, y_0) = 0$

polynomen met het goede nulpunt

gegeven: polynoom $f(x, y)$
met onbekend nulpunt $(x_0, y_0) \pmod{e}$

gezocht: modulus M en polynomen $g(x, y)$
met (x_0, y_0) als nulpunt $\pmod{M}$

neem $M = e^2$ en polynomen
$e^2, \quad e \cdot f(x, y), \quad f(x, y)^2$
en sommige hiervan ook nog $\cdot x, \cdot x^2, \cdot y$

welke precies: geheim van de smid ☺

om precies te zijn

$$g_{0,0}(x,y) = e^2$$
$$g_{1,0}(x,y) = e^2 \cdot x$$
$$g_{0,1}(x,y) = e \cdot f(x,y)$$
$$g_{2,0}(x,y) = e^2 \cdot x^2$$
$$g_{1,1}(x,y) = e \cdot x \cdot f(x,y)$$
$$g_{0,2}(x,y) = f(x,y)^2$$
$$h_{1,0}(x,y) = e^2 \cdot y$$
$$h_{1,1}(x,y) = e \cdot y \cdot f(x,y)$$
$$h_{1,2}(x,y) = y \cdot f(x,y)^2$$

hun coëfficiënten

	1	x	xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
$g_{0,0}$	e^2								
$g_{1,0}$		e^2							
$g_{0,1}$	$-e$	$-e(n+1)$	e						
$g_{2,0}$				e^2					
$g_{1,1}$		$-e$		$-e(n+1)$	e				
$g_{0,2}$	1	$2(n+1)$	-2	$(n+1)^2$	$-2(n+1)$	1			
$h_{1,0}$							e^2		
$h_{1,1}$			$-e(n+1)$				$-e$	e	
$h_{1,2}$			$2(n+1)$		$(n+1)^2$	$-2(n+1)$		-2	1

neem nu combinaties van polynomen
= combinaties van rijen in deze tabel
zodat de getallen erin kleiner worden

techniek: roosterbasisreductie, LLL

hoe nu het nulpunt vinden?

techniek: resultante

kies twee polynomen die vermoedelijk goed zijn:

$$p_1(x,y) = b_1(y) + c_1(y)\cdot x + d_1(y)\cdot x^2,$$
$$p_2(x,y) = b_2(y) + c_2(y)\cdot x + d_2(y)\cdot x^2$$

zoek een combinatie waar de x uit verdwenen is:

$$a_1 = -d_2\cdot(b_1\cdot d_2 - b_2\cdot d_1) + (c_2 + d_2\cdot x)\cdot(c_1\cdot d_2 - c_2\cdot d_1),$$
$$a_2 = d_1\cdot(b_1\cdot d_2 - b_2\cdot d_1) - (c_1 + d_1\cdot x)(c_1\cdot d_2 - c_2\cdot d_1)$$

dan voldoet

$$a_1(x,y)\cdot p_1(x,y) + a_2(x,y)\cdot p_2(x,y)$$

factoriseren

dus het polynoom

$a_1(x,y) \cdot p_1(x,y) + a_2(x,y) \cdot p_2(x,y)$

hangt alléén van y af

en heeft dus y_0 als nulpunt

die is makkelijk te vinden (numerieke methoden)

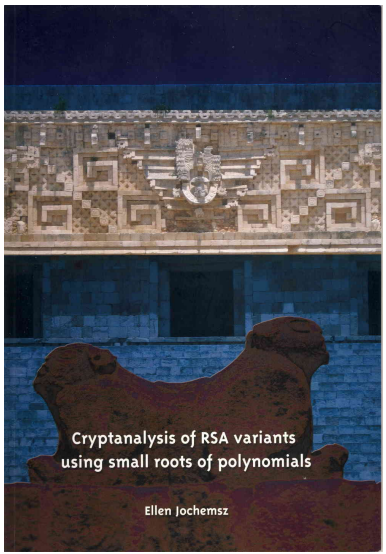
$y_0 = p + q$ is nu bekend

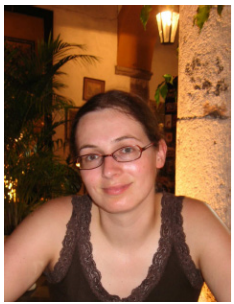
dus p en q zijn makkelijk te vinden

conclusie

deze techniek werkt voor d tot aan $n^{0.292}$

allerlei varianten zijn te verzinnen
zie proefschrift dr. Ellen Jochemsz, TU/e 2007





factoriseren met een hint

stel van p is de bovenste helft van de cijfers gelekt

dan weet je ze ook van q

Coppersmith: dan kun je heel p en q berekenen

dus $p = p_0 + x_0$, $q = q_0 + y_0$,
met $|x_0|, |y_0| < X \approx \sqrt[4]{n}$

$(p_0 + x_0) \cdot (q_0 + y_0) = n$
geeft polynoom met klein nulpunt (x_0, y_0):
$f^*(x, y) = x \cdot y + q_0 \cdot x + p_0 \cdot y + (p_0 \cdot q_0 - n)$

vergelijkbare technieken

kies (slim) modulus M

en vermenigvuldig $f^*(x,y)$ met een c

zodat de constante term $1 \pmod M$ wordt:

$$f(x,y) = 1 + a \cdot y + b \cdot x + c \cdot x \cdot y$$

nu is

$$f(x_0,y_0) \equiv c \cdot f^*(x_0,y_0) = 0 \pmod M$$

iets andere keuze polynomen

$$g_{0,0}(x,y) = X^4 \cdot f(x,y)$$
$$g_{1,0}(x,y) = X^3 \cdot x \cdot f(x,y)$$
$$g_{0,1}(x,y) = X^3 \cdot y \cdot f(x,y)$$
$$g_{1,1}(x,y) = X^2 \cdot x \cdot y \cdot f(x,y)$$
$$h_{2,0}(x,y) = M \cdot x^2$$
$$h_{0,2}(x,y) = M \cdot y^2$$
$$h_{2,1}(x,y) = M \cdot x^2 \cdot y$$
$$h_{1,2}(x,y) = M \cdot x^2 \cdot y$$
$$h_{2,2}(x,y) = M \cdot x^2 \cdot y^2$$

dan blijkt het te lukken

	1	x	y	xy	x^2	y^2	x^2y	xy^2	x^2y^2
$g_{0,0}$	X^4	aX^4	bX^4	cX^4					
$g_{1,0}$		X^3		bX^3	aX^3		cX^3		
$g_{0,1}$			X^3	aX^3		bX^3		cX^3	
$g_{1,1}$				X^2			aX^2	bX^2	cX^2
$h_{2,0}$					M				
$h_{0,2}$						M			
$h_{2,1}$							M		
$h_{1,2}$								M	
$h_{2,2}$									M

roosterbasisreductie met LLL doen

selecteer één polynoom p_1

bereken resultante van p_1 met f^*

en los de zaak op

de magnetron-aanval

RSA met CRT: sneller ontsleutelen

in plaats van d nu gebruiken:

$d_p \equiv d \pmod{(p-1)}$,

$d_q \equiv d \pmod{(q-1)}$

u zodat $p \cdot u \equiv 1 \pmod{q}$

ontsleutelen: apart $\pmod{p}$ en $\pmod{q}$:

$m_p \equiv c^{d_p} \pmod{p}$,

$m_q \equiv c^{d_q} \pmod{q}$,

$m \equiv m_p + p \cdot u \cdot (m_q - m_p) \pmod{n}$

een fout aanbrengen

smartcard bevat privé-sleutel in CRT-vorm

veronderstel: d_p is veranderd in d'_p

(hoeft maar één bit anders te zijn)
maar verder blijft alles hetzelfde

dan kan een aanvaller de volledige privé-sleutel
uit de smartcard halen

de aanval

kies een willekeurige m

versleutel deze (op je PC) met de publieke sleutel:

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

voer c aan de smartcard voor ontsleuteling,
deze berekening wordt:

$$m'_p \equiv c^{d'_p} \pmod{p},$$

$$m_q \equiv c^{d_q} \pmod{q},$$

$$m' \equiv m'_p + p \cdot u \cdot (m_q - m'_p) \pmod{n}$$

de aanval, vervolg

nu is $m' \equiv m_q \pmod{q}$ nog wel goed,
maar $m' \equiv m'_p \pmod{p}$ is fout

dus $m' \equiv m \pmod{q}$,
en $m' \not\equiv m \pmod{p}$

dus is $m - m'$ wel deelbaar door q,
maar niet meer deelbaar door p

de aanval, slot

dan hebben n en $m - m'$ dus q als gemeenschappelijke deler, maar niet p

en dan lekt q direct door ggd$(m - m', n)$ te berekenen