CRYPTANALYSIS OF RSA USING THE RATIO OF THE PRIMES

Abderrahmane NITAJ

LMNO, Université de Caen, France

Tunis, June 24, 2009

تونس، إفريقيا

Colour conventions

Red

Secret parameters.

Blue or Black

Public parameters.

Colour conventions

Red

Secret parameters.

Blue or Black

Public parameters.

RSA cryptosystem

- Invented by Rivest, Shamir and Adleman in 1977.
- The world's successful public key encryption algorithm.
- The security of RSA is based on the problem of factoring large integers: Given $N = pq$, find p and q.
- p and q are large primes (at least 512 bits).

The RSA modulus

- p, q large primes of equal bitsize.
- $N = pq$ is the RSA modulus.

The public and private exponents

- $\phi(N) = (p-1)(q-1)$, the Euler totient function.
- $e \in \mathbb{N}$, with $1 < e < \phi(N)$, and $\gcd(e, \phi(N)) = 1$, the public exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.

The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

The attacks

Given N, e, find p, q.

The RSA modulus

- p, q large primes of equal bitsize.
- $N = pq$ is the RSA modulus.

The public and private exponents

- $\phi(N) = (p-1)(q-1)$, the Euler totient function.
- $e \in \mathbb{N}$, with $1 < e < \phi(N)$, and $\gcd(e, \phi(N)) = 1$, the public exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.

The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

The attacks

Given N, e, find p, q.

The RSA modulus

- p, q large primes of equal bitsize.
- $N = pq$ is the RSA modulus.

The public and private exponents

- $\phi(N) = (p-1)(q-1)$, the Euler totient function.
- $e \in \mathbb{N}$, with $1 < e < \phi(N)$, and $\gcd(e, \phi(N)) = 1$, the public exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.

The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

The attacks

Given N, e, find p, q.

The RSA modulus

- p, q large primes of equal bitsize.
- $N = pq$ is the RSA modulus.

The public and private exponents

- $\phi(N) = (p-1)(q-1)$, the Euler totient function.
- $e \in \mathbb{N}$, with $1 < e < \phi(N)$, and $\gcd(e, \phi(N)) = 1$, the public exponent.
- $ed \equiv 1 \pmod{\phi(N)}$.
- $d \in \mathbb{N}$, $1 < d < \phi(N)$, the private exponent.

The RSA equation

$$ed - (p-1)(q-1)k = 1.$$

The attacks

Given N, e, find p, q.

Wiener

Using the RSA equation

$$ed-(p-1)(q-1)k=1.$$

Wiener, 1990

If $d<\frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N=pq$ can be found.

The method

- $\frac{k}{d}\approx\frac{e}{N}$.
- The continued fraction algorithm.

Wiener

Using the RSA equation

$$ed - (p-1)(q-1)k = 1.$$

Wiener, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

Wiener

Using the RSA equation

$$ed - (p-1)(q-1)k = 1.$$

Wiener, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

Boneh-Durfee

Using the RSA equation

$$ed - (p-1)(q-1)k = 1.$$

Boneh-Durfee, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p + q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Boneh-Durfee

Using the RSA equation

$$ed - (p-1)(q-1)k = 1.$$

Boneh-Durfee, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p+q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Boneh-Durfee

Using the RSA equation

$$ed - (p-1)(q-1)k = 1.$$

Boneh-Durfee, 2000

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p+q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Blömer-May

Using a variant of the RSA equation

$$ex - (p-1)(q-1)k = y.$$

Blömer-May, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Blömer-May

Using a variant of the RSA equation

$$ex - (p-1)(q-1)k = y.$$

Blömer-May, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Blömer-May

Using a variant of the RSA equation

$$ex - (p-1)(q-1)k = y.$$

Blömer-May, 2004

If $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| = O\left(N^{-\frac{3}{4}}ex\right)$ then the factorization of $N = pq$ can be found.

The method

- $\frac{k}{x} \approx \frac{e}{N}$.
- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Nitaj

Using a variant of the RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

$u = v = 1$ implies the RSA equation $ed - (p-1)(q-1)k = 1$.

Nitaj, 2008

If $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[-\frac{qu}{p-u} \right]$, and all prime factors of $p-u$ or $q-v$ are less than 10^{50}, then the factorization of $N = pq$ can be found.

The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Nitaj

Using a variant of the RSA equation

$$eX-(p-u)(q-v)Y=1.$$

$u=v=1$ implies the RSA equation $ed-(p-1)(q-1)k=1$.

Nitaj, 2008

If $1\leq Y<X<2^{-\frac{1}{4}}N^{\frac{1}{4}},\ |u|<N^{\frac{1}{4}},\ v=\left[-\frac{qu}{p-u}\right]$, and all prime factors of $p-u$ or $q-v$ are less than 10^{50}, then the factorization of $N=pq$ can be found.

The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Nitaj

Using a variant of the RSA equation

$$eX - (p-u)(q-v)Y = 1.$$

$u = v = 1$ implies the RSA equation $ed - (p-1)(q-1)k = 1$.

Nitaj, 2008

If $1 \leq Y < X < 2^{-\frac{1}{4}} N^{\frac{1}{4}}$, $|u| < N^{\frac{1}{4}}$, $v = \left[-\frac{qu}{p-u}\right]$, and all prime factors of $p-u$ or $q-v$ are less than 10^{50}, then the factorization of $N = pq$ can be found.

The method

- The continued fraction algorithm.
- H.W. Lenstra's elliptic curve method (ECM).
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

The new attacks

The variant RSA equation

$eX - (N - (ap + bq))Y = Z$, where $\frac{a}{b}$ is a convergent of $\frac{q}{p}$

If $a = b = 1$, then $eX - (p-1)(q-1)Y = Z - Y$ (Blömer-May).

The attacks

1. Small Difference $|ap - bq| < (abN)^{\frac{1}{4}}$
2. Medium Difference $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
3. Large Difference $aN^{\frac{1}{4}} < |ap - bq|$

The method

- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.
- H.W. Lenstra's elliptic curve method (ECM).

The new attacks

The variant RSA equation

$eX - (N - (ap + bq))Y = Z$, where $\frac{a}{b}$ is a convergent of $\frac{q}{p}$

If $a = b = 1$, then $eX - (p-1)(q-1)Y = Z - Y$ (Blömer-May).

The attacks

1. Small Difference $|ap - bq| < (abN)^{\frac{1}{4}}$
2. Medium Difference $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
3. Large Difference $aN^{\frac{1}{4}} < |ap - bq|$

The method

- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.
- H.W. Lenstra's elliptic curve method (ECM).

The new attacks

The variant RSA equation

$eX - (N - (ap + bq))Y = Z$, where $\frac{a}{b}$ is a convergent of $\frac{q}{p}$

If $a = b = 1$, then $eX - (p-1)(q-1)Y = Z - Y$ (Blömer-May).

The attacks

1. Small Difference $|ap - bq| < (abN)^{\frac{1}{4}}$
2. Medium Difference $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
3. Large Difference $aN^{\frac{1}{4}} < |ap - bq|$

The method

- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.
- H.W. Lenstra's elliptic curve method (ECM).

The new attacks

The variant RSA equation

$eX - (N - (ap + bq))Y = Z$, where $\frac{a}{b}$ is a convergent of $\frac{q}{p}$

If $a = b = 1$, then $eX - (p-1)(q-1)Y = Z - Y$ (Blömer-May).

The attacks

1. Small Difference $|ap - bq| < (abN)^{\frac{1}{4}}$
2. Medium Difference $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
3. Large Difference $aN^{\frac{1}{4}} < |ap - bq|$

The method

- The continued fraction algorithm.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.
- H.W. Lenstra's elliptic curve method (ECM).

Continued fractions

The Continued fraction alorithm

- e and N are coprime positive integers.
- $$\frac{e}{N} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}.$$
- $\frac{e}{N} = [a_0, a_1, a_2, \cdots]$ where a_i are positive integers.
- $\frac{r_i}{s_i} = [a_0, a_1, a_2, \cdots, a_i]$ are called the convergents.

Continued fractions

Theorem

If $\frac{a}{b}$ is a convergent of x, then

$$\left|x-\frac{a}{b}\right|<\frac{1}{b^2}.$$

Theorem

If

$$\left|x-\frac{a}{b}\right|<\frac{1}{2b^2},$$

then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion of x.

Continued fractions

Theorem

If $\frac{a}{b}$ is a convergent of x, then

$$\left|x - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Theorem

If

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion of x.

Coppersmith's method

Coppermith's Theorem

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Given an approximation $\tilde{p}$ of p with $|p - \tilde{p}| < N^{\frac{1}{4}}$, then $N = pq$ can be factored in time polynomial in $\log N$.

Coppermith's Theorem

- Lattices
- Lenstra-Lenstra-Lovasz (LLL) algorithm

Coppersmith's method

Coppermith's Theorem

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Given an approximation $\tilde{p}$ of p with $|p - \tilde{p}| < N^{\frac{1}{4}}$, then $N = pq$ can be factored in time polynomial in $\log N$.

Coppermith's Theorem

- Lattices
- Lenstra-Lenstra-Lovasz (LLL) algorithm

ECM

Smooth numbers

Let y be a positive constant. A positive number n is y-smooth if all prime factors of n are less than y.

The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor B_{ecm}-smooth integers where

$$B_{\text{ecm}} = 10^{52}$$

ECM

Smooth numbers

Let y be a positive constant. A positive number n is y-smooth if all prime factors of n are less than y.

The Elliptic Curve Method (ECM)

- H.W. Lenstra, 1985, phase 1.
- Brent, Montgomery, 1986-87, phase 2.
- ECM is very efficient to factor B_{ecm}-smooth integers where

$$B_{\text{ecm}} = 10^{52}$$

The first attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The first attack: Small Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ with $a \geq 1$ and $|ap - bq| < (abN)^{\frac{1}{4}}$.
- Set $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - $|Z| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) Y$,

then N can be factored in polynomial time.

The first attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The first attack: Small Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ with $a \geq 1$ and $|ap - bq| < (abN)^{\frac{1}{4}}$.
- Set $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - $|Z| < \inf\left((abN)^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right) Y$,

  then N can be factored in polynomial time.

The second attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The second attack: Medium Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that
  - $a \geq 1$, $b \leq 10^{52}$
  - $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
- Set $M = N - \frac{eX}{Y}$ and $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - and $|Z| < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$,

  then, under ECM, N can be factored efficiently.

The second attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The second attack: Medium Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that
  - $a \geq 1$, $b \leq 10^{52}$
  - $(abN)^{\frac{1}{4}} < |ap - bq| < aN^{\frac{1}{4}}$
- Set $M = N - \frac{eX}{Y}$ and $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - and $|Z| < \min\left(aN^{\frac{1}{4}}, \frac{1}{2}N^{\frac{1}{2}-\alpha}\right)Y$,

then, under ECM, N can be factored efficiently.

The third attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The third attack: Large Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that $a \geq 1$ and $b \leq 10^{52}$.
- Set $M = N - \frac{eX}{Y}$, $D = \sqrt{|M^2 - 4abN|}$
- $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - and $|Z| < \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}Y$

  then, under ECM, N can be factored efficiently.

The third attack

The variant RSA equation

$$eX - (N - (ap + bq))Y = Z.$$

The third attack: Large Difference $|ap - bq|$

- Let $\frac{a}{b}$ be an unknown convergent of the continued fraction expansion of $\frac{q}{p}$ such that $a \geq 1$ and $b \leq 10^{52}$.
- Set $M = N - \frac{eX}{Y}$, $D = \sqrt{|M^2 - 4abN|}$
- $ap + bq = N^{\frac{1}{2}+\alpha}$ with $0 < \alpha < \frac{1}{2}$.
- If
  - $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}-\frac{\alpha}{2}}$
  - and $|Z| < \frac{1}{3}a|ap - bq|N^{-\frac{1}{4}-\alpha}Y$

then, under ECM, N can be factored efficiently.

The proofs in brief

Using the equation $eX - (N - (ap + bq))Y = Z$.

- Write $eX - NY = Z - (ap + bq)Y$. Then, if X, Y and Z are "small", we get

$$\frac{Y}{X} \approx \frac{e}{N}.$$

- Compute X, Y from **the continued fraction expansion** of $\frac{e}{N}$.
- Hence $ap + bq = N - \frac{eX}{Y} + \frac{Z}{Y}$ and if $\frac{|Z|}{Y}$ is "small", then $ap + bq \approx N - \frac{eX}{Y}$ and

$$ab = \left[\frac{\left(N - \frac{eX}{Y}\right)^2}{4N} \right].$$

The proofs in brief

Using the equation $eX-(N-(ap+bq))Y=Z$.

- Write $eX-NY=Z-(ap+bq)Y$. Then, if X, Y and Z are "small", we get
$$\frac{Y}{X}\approx\frac{e}{N}.$$
- Compute X, Y from **the continued fraction expansion** of $\frac{e}{N}$.
- Hence $ap+bq=N-\frac{eX}{Y}+\frac{Z}{Y}$ and if $\frac{|Z|}{Y}$ is "small", then $ap+bq\approx N-\frac{eX}{Y}$ and
$$ab=\left[\frac{\left(N-\frac{eX}{Y}\right)^2}{4N}\right].$$

The proofs in brief

Using the equation $eX-(N-(ap+bq))Y=Z$.

- Write $eX-NY=Z-(ap+bq)Y$. Then, if X, Y and Z are "small", we get
$$\frac{Y}{X}\approx\frac{e}{N}.$$
- Compute X, Y from **the continued fraction expansion** of $\frac{e}{N}$.
- Hence $ap+bq=N-\frac{eX}{Y}+\frac{Z}{Y}$ and if $\frac{|Z|}{Y}$ is "small", then $ap+bq\approx N-\frac{eX}{Y}$ and
$$ab=\left[\frac{\left(N-\frac{eX}{Y}\right)^2}{4N}\right].$$

The first attack

If $|ap - bq|$ is “small”, then

$$\left| ap - \frac{N - \frac{eX}{Y}}{2} \right| \leq (abN)^{\frac{1}{4}}.$$

Hence $ap \approx \frac{N - \frac{eX}{Y}}{2}$ and applying Copersmith’s theorem, we find ap and finally $p = gcd(ap, N)$.

The second attack

If $|ap - bq|$ is "medium" and $b < 10^{52}$, then

- Apply ECM to find a, b with $a < b < 2a$ using $ab = \left[\frac{\left(N - \frac{eX}{Y}\right)^2}{4N}\right]$.
- Hence
$$\left| p - \frac{N - \frac{eX}{Y}}{2a} \right| \leq N^{\frac{1}{4}}.$$

Hence $p \approx \frac{N - \frac{eX}{Y}}{2a}$ and applying Copersmith's theorem, we find p.

The third attack

If $|ap - bq|$ is "large" and $b < 10^{52}$, then

- Apply ECM to find a, b with $a < b < 2a$ using $ab = \left[\frac{\left(N-\frac{eX}{Y}\right)^2}{4N}\right]$.
- Compute $D = \sqrt{|M^2 - 4abN|}$.
- Hence

$$\left|p - \frac{D + N - \frac{eX}{Y}}{2a}\right| \leq N^{\frac{1}{4}}.$$

Hence $p \approx \frac{D+N-\frac{eX}{Y}}{2a}$ and applying Copersmith's theorem, we find p.

Cardinality

- $eX - (N - (ap + bq))Y = Z$.
- The parameters X, Y, Z are “small”.
- $\frac{a}{b}$ is a convergente of $\frac{q}{p}$.
- Then using the continued fraction algoritm, ECM and Cppersmit’s method, we can find the factorization of $N = pq$.
- The number of such week keys is at least $N^{\frac{3}{4}-\varepsilon}$.

Thank you for your attention

Merci

شكرا