RSA VI

Square roots mod n and Dixon's method of random squares

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

What other numbers are easy to factor?

Take $n = 323$

What other numbers are easy to factor?

Take $n = 323$ and note
$323 = 324 - 1$

What other numbers are easy to factor?

Take $n = 323$ and note
$323 = 324 - 1 = 18^2 - 1$

What other numbers are easy to factor?

Take $n = 323$ and note
$323 = 324 - 1 = 18^2 - 1 = (18 - 1)(18 + 1) = 17 \cdot 19.$

What other numbers are easy to factor?

Take $n = 323$ and note
$323 = 324 - 1 = 18^2 - 1 = (18 - 1)(18 + 1) = 17 \cdot 19.$

Notice this by computing $\sqrt{n}$, here $\sqrt{323} = 17.97\ldots$,
and observing that it is close to an integer.

Then try dividing n by $\lfloor \sqrt{n} \rfloor, \lfloor \sqrt{n} \rfloor - 1, \lfloor \sqrt{n} \rfloor - 2, \lfloor \sqrt{n} \rfloor - 3, \ldots$

This degrades into factorization by trial division, so works for any n but is efficient only for n of the form $n = a^2 - b^2$ for small b.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get

$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$

with $a \not\equiv \pm b \bmod n$ then

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get

$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$

with $a \not\equiv \pm b \bmod n$ then $\gcd(a-b, n)$ is a nontrivial factor of n.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get

$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$

with $a \not\equiv \pm b \bmod n$ then $\gcd(a-b, n)$ is a nontrivial factor of n.

Pick random $1 < a < n$, let $c \equiv a^2 \bmod n$, ask A for square root of c.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get
$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$
with $a \not\equiv \pm b \bmod n$ then $\gcd(a-b, n)$ is a nontrivial factor of n.

Pick random $1 < a < n$, let $c \equiv a^2 \bmod n$, ask A for square root of c.

With $> 50\%$ probability (see video and slides for Miller–Rabin test) $a \not\equiv \pm b \bmod n$ and $\gcd(a-b, n)$ factors n. Repeat if necessary.

We have now reduced computing square roots mod n to factoring n.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get
$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$
with $a \not\equiv \pm b \bmod n$ then $\gcd(a-b, n)$ is a nontrivial factor of n.

Pick random $1 < a < n$, let $c \equiv a^2 \bmod n$, ask A for square root of c.

With $> 50\%$ probability (see video and slides for Miller–Rabin test) $a \not\equiv \pm b \bmod n$ and $\gcd(a-b, n)$ factors n. Repeat if necessary.

We have now reduced computing square roots mod n to factoring n.

Computing square roots modulo prime powers is easy, see Tonelli–Shanks in general. Even faster for special cases: For $p \equiv 3 \bmod 4$ we get $b \equiv c^{(p+1)/4} \bmod p$ as $b^2 \equiv c^{(p+1)/2} \equiv c^{(p-1)/2} c \equiv c \bmod p$.

Combine results using CRT to compute square roots modulo n.

Computing square roots mod n is equivalent to factoring n

Assume we are given an algorithm A which upon input $c \in \mathbf{Z}/n$ returns b with $c \equiv b^2 \bmod n$ if such b exists.

If we can get

$$a^2 \equiv b^2 \bmod n \Leftrightarrow a^2 - b^2 \equiv 0 \bmod n$$

with $a \not\equiv \pm b \bmod n$ then $\gcd(a-b, n)$ is a nontrivial factor of n.

Pick random $1 < a < n$, let $c \equiv a^2 \bmod n$, ask A for square root of c.

With $> 50\%$ probability (see video and slides for Miller–Rabin test) $a \not\equiv \pm b \bmod n$ and $\gcd(a-b, n)$ factors n. Repeat if necessary.

We have now reduced computing square roots mod n to factoring n.

Computing square roots modulo prime powers is easy, see Tonelli–Shanks in general. Even faster for special cases: For $p \equiv 3 \bmod 4$ we get $b \equiv c^{(p+1)/4} \bmod p$ as $b^2 \equiv c^{(p+1)/2} \equiv c^{(p-1)/2} c \equiv c \bmod p$.

Combine results using CRT to compute square roots modulo n.

Having shown both sides of the reduction, the problems are equivalent.

How to use this?

Unlikely to find $0 < a, b < n$ with $a^2 \equiv b^2 \bmod n$ by chance.

To try to build b:

How to use this?

Unlikely to find $0 < a, b < n$ with $a^2 \equiv b^2 \bmod n$ by chance.
To try to build b:

Pick random a_i, compute $c_i = (a_i^2 \bmod n) \in [0, n-1]$ and try to factor this over $\mathbf{Z}$. Obtain relation

$$c_i = \prod p_j^{e_{i,j}}.$$

How to use this?

Unlikely to find $0 < a, b < n$ with $a^2 \equiv b^2 \bmod n$ by chance.
To try to build b:

Pick random a_i, compute $c_i = (a_i^2 \bmod n) \in [0, n-1]$ and try to factor this over $\mathbf{Z}$. Obtain relation

$$c_i = \prod p_j^{e_{i,j}}.$$

Hope to find some product of c_is that give even exponents on the right.
Note: do not reduce mod n when computing this product!

How to use this?

Unlikely to find $0 < a, b < n$ with $a^2 \equiv b^2 \bmod n$ by chance.
To try to build b:

Pick random a_i, compute $c_i = (a_i^2 \bmod n) \in [0, n-1]$ and try to factor this over $\mathbf{Z}$. Obtain relation

$$c_i = \prod p_j^{e_{i,j}}.$$

Hope to find some product of c_is that give even exponents on the right.
Note: do not reduce mod n when computing this product!

If $\prod c_i$ has even exponents for all p_j then

$$\prod_i a_i^2 \equiv \prod_j p_j^{2e_j} \bmod n$$

and we have our desired equivalence of squares.

How to use this?

Unlikely to find $0 < a, b < n$ with $a^2 \equiv b^2 \bmod n$ by chance.
To try to build b:

Pick random a_i, compute $c_i = (a_i^2 \bmod n) \in [0, n-1]$ and try to factor this over $\mathbf{Z}$. Obtain relation

$$c_i = \prod p_j^{e_{i,j}}.$$

Hope to find some product of c_is that give even exponents on the right.
Note: do not reduce mod n when computing this product!

If $\prod c_i$ has even exponents for all p_j then

$$\prod_i a_i^2 \equiv \prod_j p_j^{2e_j} \bmod n$$

and we have our desired equivalence of squares.

Large p_j are less likely to appear twice. Define factor base

$$\mathcal{F} = \{p_j | p_j \text{ prime }, p_j < B\}$$

for some bound B.
Store relations for c_i that factor completely over $\mathcal{F}$, i.e., are B-smooth.

Example

Factor $n = 299$.
$96^2 \equiv 246 \bmod n$; $\quad 246 = 2 \cdot 3 \cdot 41$

96	|	2	3	41

Example

Factor $n = 299$.
$91^2 \equiv 208 \bmod n; \quad 208 = 2^4 \cdot 13$

96	2	3			41
91	2^4			13	

Example

Factor $n = 299$.
$89^2 \equiv 147 \bmod n; \quad 147 = 3 \cdot 7^2$

96	2	3			41
91	2^4			13	
89		3	7^2		

Example

Factor $n = 299$.
$69^2 \equiv 276 \bmod n; \quad 276 = 2^2 \cdot 3 \cdot 23$

96	2	3				41
91	2^4			13		
89		3	7^2			
69	2^2	3			23	

Example

Factor $n = 299$.
$23^2 \equiv 230 \bmod n; \quad 230 = 2 \cdot 5 \cdot 23$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	

Example

Factor $n = 299$.
$25^2 \equiv 27 \bmod n; \quad 27 = 3^3$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	
25		3^3					

Example

Factor $n = 299$.
$25^2 \equiv 27 \bmod n; \quad 27 = 3^3$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	
25		3^3					

$(89 \cdot 25)^2 \equiv 3^4 \cdot 7^2 = (3^2 \cdot 7)^2 \bmod 299$

Example

Factor $n = 299$.
$25^2 \equiv 27 \bmod n; \quad 27 = 3^3$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	
25		3^3					

$(89 \cdot 25)^2 \equiv 3^4 \cdot 7^2 = (3^2 \cdot 7)^2 \bmod 299$ and $\gcd(89 \cdot 25 - 9 \cdot 7, 299) = 23$.

Example

Factor $n = 299$.
$25^2 \equiv 27 \bmod n; \quad 27 = 3^3$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	
25		3^3					

$(89 \cdot 25)^2 \equiv 3^4 \cdot 7^2 = (3^2 \cdot 7)^2 \bmod 299$ and $\gcd(89 \cdot 25 - 9 \cdot 7, 299) = 23$.

Note: Small examples have wrong distribution, e.g.,
$85^2 \equiv 49 \bmod 299$ factors 299 instantly;
$73^2 \equiv 246 \bmod 299, \quad 246 = 2 \cdot 3 \cdot 41$ gives complete match with 96^2,
even though 41 very unlikely to reappear.

Example

Factor $n = 299$.
$25^2 \equiv 27 \bmod n; \quad 27 = 3^3$

96	2	3					41
91	2^4				13		
89		3		7^2			
69	2^2	3				23	
23	2		5			23	
25		3^3					

$(89 \cdot 25)^2 \equiv 3^4 \cdot 7^2 = (3^2 \cdot 7)^2 \bmod 299$ and $\gcd(89 \cdot 25 - 9 \cdot 7, 299) = 23$.

Note: Small examples have wrong distribution, e.g.,
$85^2 \equiv 49 \bmod 299$ factors 299 instantly;
$73^2 \equiv 246 \bmod 299, \quad 246 = 2 \cdot 3 \cdot 41$ gives complete match with 96^2,
even though 41 very unlikely to reappear.

For bigger sizes, store only exponents on right-hand side, consider matrix over $\mathbf{F}_2$ to find relation.

Factorization using equivalence of squares

Target: odd integer n, want to factor it.

1. Fix a factor base $\mathcal{F}$ of small primes. Let $f = |\mathcal{F}|$.
2. Repeat the following until $f + 4$ relations are collected.
   2.1 Pick random integer a.
   2.2 Compute $c \equiv a^2 \bmod n$ with $c \in [0, n-1]$.
   2.3 Check whether c factors over the factor base, i.e. whether

   $$c = \prod_{i=1}^{f} pi^{e_i} \text{ for } p_i \in \mathcal{F}, e_i \in \mathbf{N}$$

   If so, store relation $(a, [e_1, e_2, \ldots, e_f])$
3. Put the exponents-part of the relations in a matrix, compute a non-zero vector in the kernel of the matrix modulo 2.
   If the matrix has no non-trivial vector, go back to collecting more relations.
4. Put A the product of all a involved in the kernel vector (non-zero entries).
   Compute the product of all prime powers involved in the kernel vector. All exponents are even, put B the square root.
   Compute $\gcd(A - B, n)$.