Math 134: Cryptography

Lecture 9: Choosing primes for RSA

Eoin Mackall

January 27, 2025

University of California, Santa Cruz

Last Time

Last time

We ended last time arguing that the security of RSA encryption is closely related to the problem of integer factorization:

Integer Factorization Problem

Let $n > 1$ be an integer. Find a prime p that divides n.

Last time

We ended last time arguing that the security of RSA encryption is closely related to the problem of integer factorization:

Integer Factorization Problem

Let $n > 1$ be an integer. Find a prime p that divides n.

Example (One solution)

Long division of an integer n with d digits in its binary expansion by an integer with $d/2$ binary digits requires $\mathcal{O}(d^2)$ bit operations.

Last time

We ended last time arguing that the security of RSA encryption is closely related to the problem of integer factorization:

Integer Factorization Problem

Let $n > 1$ be an integer. Find a prime p that divides n.

Example (One solution)

Long division of an integer n with d digits in its binary expansion by an integer with $d/2$ binary digits requires $\mathcal{O}(d^2)$ bit operations.

We could try to divide to divide n by $1, 2, \ldots, \sqrt{n}$. If n is composite, then there will be a prime number in this list.

Last time

We ended last time arguing that the security of RSA encryption is closely related to the problem of integer factorization:

Integer Factorization Problem

Let $n > 1$ be an integer. Find a prime p that divides n.

Example (One solution)

Long division of an integer n with d digits in its binary expansion by an integer with $d/2$ binary digits requires $\mathcal{O}(d^2)$ bit operations.

We could try to divide to divide n by $1, 2, \ldots, \sqrt{n}$. If n is composite, then there will be a prime number in this list.

If there are d digits in the binary expansion of n, then

$$2^{d-1} \leq n < 2^d.$$

So this requires performing approximately $2^{d/2} = \sqrt{2^d}$ divisions, giving $\mathcal{O}(2^{d/2}d^2)$ bit operations in total.

Last time

There are more advanced methods for factoring integers (e.g. the quadratic or number field sieve, Pollard's rho algorithm, elliptic curve factorization).

Last time

There are more advanced methods for factoring integers (e.g. the quadratic or number field sieve, Pollard's rho algorithm, elliptic curve factorization).

Some of these work with subexponential time complexity (e.g. like $\mathcal{O}(2^{\sqrt{d \log(d)}})$ on integers n with d binary digits).

Last time

There are more advanced methods for factoring integers (e.g. the quadratic or number field sieve, Pollard's rho algorithm, elliptic curve factorization).

Some of these work with subexponential time complexity (e.g. like $\mathcal{O}(2^{\sqrt{d \log(d)}})$ on integers n with d binary digits).

In general, all of these algorithms have some difficulty factoring large integers on modern computers.

Table of contents

Primality Tests

Primality tests

We'll start with the following problem:

Primality Decision Problem

Let $n > 1$ be an integer. Determine if n is prime or composite.

Primality tests

We'll start with the following problem:

Primality Decision Problem

Let $n > 1$ be an integer. Determine if n is prime or composite.

Definition

An algorithm that solves the Primality Decision Problem is called a primality test.

Primality tests

We'll start with the following problem:

Primality Decision Problem

Let $n > 1$ be an integer. Determine if n is prime or composite.

Definition

An algorithm that solves the Primality Decision Problem is called a primality test.

Any algorithm that solves the Integer Factorization Problem also gives a solution to the Primality Decision Problem.

Primality tests

We'll start with the following problem:

Primality Decision Problem

Let $n > 1$ be an integer. Determine if n is prime or composite.

Definition

An algorithm that solves the Primality Decision Problem is called a primality test.

Any algorithm that solves the Integer Factorization Problem also gives a solution to the Primality Decision Problem.

However, it's often easier to test for primality than it is to find a factorization of a given integer.

Fermat Primality Test

Recall the theorem:

Theorem (Fermat's Little Theorem)

Let p be a prime number. Then for any integer $a \in \mathbb{Z}$ with $p \nmid a$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat Primality Test

Recall the theorem:

Theorem (Fermat's Little Theorem)

Let p be a prime number. Then for any integer $a \in \mathbb{Z}$ with $p \nmid a$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Using this we can get the following:

Fermat Primality Test

Let $n > 1$ be an integer. Suppose that there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

Then n is composite.

Fermat Primality Test

Fermat Primality Test

Let $n > 1$ be an integer. Suppose that there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

Then n is composite.

Fermat Primality Test

Let $n > 1$ be an integer. Suppose that there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

Then n is composite.

Remark

Note that if there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, then we have determined that n is composite without having determined a proper divisor of n.

Fermat Primality Test

Let $n > 1$ be an integer. Suppose that there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

Then n is composite.

Remark

Note that if there exists an integer $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, then we have determined that n is composite without having determined a proper divisor of n.

Remark

Strictly speaking, the Fermat Primality Test does not solve the Primality Decision Problem. Notably, if we find an integer a with $a^{n-1} \equiv 1 \pmod{n}$ then we can not determine that n is prime.

Fermat Primality Test

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$3^2 \equiv 9 \pmod{33}$$

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$\begin{aligned} 3^2 &\equiv 9 && \pmod{33} \\ 3^4 &\equiv 81 \equiv 81 - 2 \cdot (33) \equiv 15 && \pmod{33} \end{aligned}$$

Fermat Primality Test

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$\begin{aligned} 3^2 &\equiv 9 &&\pmod{33} \\ 3^4 &\equiv 81 \equiv 81 - 2 \cdot (33) \equiv 15 &&\pmod{33} \\ 3^8 &\equiv 225 \equiv 225 - 6 \cdot (33) \equiv 27 &&\pmod{33} \end{aligned}$$

Fermat Primality Test

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$\begin{aligned}
3^2 &\equiv 9 && \pmod{33} \\
3^4 &\equiv 81 \equiv 81 - 2 \cdot (33) \equiv 15 && \pmod{33} \\
3^8 &\equiv 225 \equiv 225 - 6 \cdot (33) \equiv 27 && \pmod{33} \\
3^{16} &\equiv (27)^2 \equiv (-6)^2 \equiv 3 && \pmod{33}
\end{aligned}$$

Fermat Primality Test

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$\begin{aligned}
3^2 &\equiv 9 && \pmod{33} \\
3^4 &\equiv 81 \equiv 81 - 2 \cdot (33) \equiv 15 && \pmod{33} \\
3^8 &\equiv 225 \equiv 225 - 6 \cdot (33) \equiv 27 && \pmod{33} \\
3^{16} &\equiv (27)^2 \equiv (-6)^2 \equiv 3 && \pmod{33} \\
3^{32} &\equiv 9 && \pmod{33}
\end{aligned}$$

Fermat Primality Test

Example

Let $n = 33$. We have $n - 1 = 32 = 2^5$.

$$\begin{aligned}
3^2 &\equiv 9 && \pmod{33} \\
3^4 &\equiv 81 \equiv 81 - 2 \cdot (33) \equiv 15 && \pmod{33} \\
3^8 &\equiv 225 \equiv 225 - 6 \cdot (33) \equiv 27 && \pmod{33} \\
3^{16} &\equiv (27)^2 \equiv (-6)^2 \equiv 3 && \pmod{33} \\
3^{32} &\equiv 9 && \pmod{33}
\end{aligned}$$

The Fermat Primality Test implies that $n = 33$ is composite, which we knew since $33 = 3 \cdot 11$.

Fermat Primality Test

Example

Let $n = 5049$ and $a = 2$.

Fermat Primality Test

Example

Let $n = 5049$ and $a = 2$. Then

$$2^{5048} \equiv 256 \pmod{5049}$$

so $n = 5049$ is composite.

Fermat Primality Test

Example

Let $n = 5049$ and $a = 2$. Then

$$2^{5048} \equiv 256 \pmod{5049}$$

so $n = 5049$ is composite.

Example

Let $n = 561$ and let $a = 2$.

Example

Let $n = 5049$ and $a = 2$. Then

$$2^{5048} \equiv 256 \pmod{5049}$$

so $n = 5049$ is composite.

Example

Let $n = 561$ and let $a = 2$. Then

$$a^{n-1} \equiv 2^{560} \equiv 1 \pmod{561}$$

but we will see that n is composite (i.e. $n = 3 \cdot 11 \cdot 17$).

Miller-Rabin Primality Test

There is an improvement of the Fermat Primality Test called the Miller-Rabin Primality Test.

There is an improvement of the Fermat Primality Test called the Miller-Rabin Primality Test.

Before we see this improvement, we need the following lemma:

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Proof.

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Proof.

$\square$

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Proof.

Some algebraic manipulation yields

$$x^2 \equiv y^2 \pmod{n}$$

□

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x-y, n)$ gives a nontrivial factor of n.

Proof.

Some algebraic manipulation yields

$$\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x^2 - y^2 &\equiv 0 \pmod{n} \end{aligned}$$

□

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Proof.

Some algebraic manipulation yields

$$\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x^2 - y^2 &\equiv 0 \pmod{n} \\ (x - y)(x + y) &\equiv 0 \pmod{n}. \end{aligned}$$

□

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \text{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x - y, n)$ gives a nontrivial factor of n.

Proof.

Some algebraic manipulation yields

$$\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x^2 - y^2 &\equiv 0 \pmod{n} \\ (x - y)(x + y) &\equiv 0 \pmod{n}. \end{aligned}$$

Since $x \not\equiv y \pmod{n}$, we find $x - y \not\equiv 0 \pmod{n}$. So $\gcd(x - y, n) < n$.

□

Miller-Rabin Primality Test

Lemma

Let $n > 1$ be an integer and suppose that there exists $x, y \in \mathbb{Z}$ with

$$x^2 \equiv y^2 \pmod{n} \quad \textit{and} \quad x \not\equiv \pm y \pmod{n}.$$

Then n is composite and $\gcd(x-y, n)$ gives a nontrivial factor of n.

Proof.

Some algebraic manipulation yields

$$\begin{aligned} x^2 &\equiv y^2 \pmod{n} \\ x^2 - y^2 &\equiv 0 \pmod{n} \\ (x-y)(x+y) &\equiv 0 \pmod{n}. \end{aligned}$$

Since $x \not\equiv y \pmod{n}$, we find $x - y \not\equiv 0 \pmod{n}$. So $\gcd(x-y, n) < n$.

If $\gcd(x-y, n) = 1$, then we could divide to find $x + y \equiv 0 \pmod{n}$. But, since $x \not\equiv -y \pmod{n}$, we must have $x + y \not\equiv 0 \pmod{n}$. $\square$

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime.

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Let $n > 1$ *be an odd integer. Write* $n - 1 = 2^k m$ *with* $m \in \mathbb{Z}$ *odd and* $k \geq 1$*. Let* $1 < a < n - 1$ *be another integer. Set* $b_0 \equiv a^m \pmod{n}$*.*

If $b_0 \equiv \pm 1 \pmod{n}$*, then* n *is probably prime. (Fermat)*

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n.

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n. (Lemma)

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Let $n > 1$ *be an odd integer. Write* $n - 1 = 2^k m$ *with* $m \in \mathbb{Z}$ *odd and* $k \geq 1$. *Let* $1 < a < n - 1$ *be another integer. Set* $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, *then* n *is probably prime. (Fermat)*

Else, let $b_1 \equiv b_0^2 \pmod{n}$. *If* $b_1 \equiv 1 \pmod{n}$, *then* n *is composite and* $\gcd(b_0 - 1, n)$ *gives a nontrivial factor of* n. *(Lemma)*

Else, if $b_1 \equiv -1 \pmod{n}$, n *is probably prime.*

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n. (Lemma)

Else, if $b_1 \equiv -1 \pmod{n}$, n is probably prime. (Can't apply Lemma)

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n. (Lemma)

Else, if $b_1 \equiv -1 \pmod{n}$, n is probably prime. (Can't apply Lemma)
If $b_1 \not\equiv \pm 1 \pmod{n}$, set $b_2 \equiv b_1^2 \pmod{n}$.

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n. (Lemma)

Else, if $b_1 \equiv -1 \pmod{n}$, n is probably prime. (Can't apply Lemma) If $b_1 \not\equiv \pm 1 \pmod{n}$, set $b_2 \equiv b_1^2 \pmod{n}$.

If $b_2 \equiv 1 \pmod{n}$ then n is composite. If $b_2 \equiv -1 \pmod{n}$ then n is probably prime. Otherwise, set $b_3 \equiv b_2^2 \pmod{n}$.

Miller-Rabin Primality Test

Let $n > 1$ be an odd integer. Write $n - 1 = 2^k m$ with $m \in \mathbb{Z}$ odd and $k \geq 1$. Let $1 < a < n - 1$ be another integer. Set $b_0 \equiv a^m \pmod{n}$.

If $b_0 \equiv \pm 1 \pmod{n}$, then n is probably prime. (Fermat)

Else, let $b_1 \equiv b_0^2 \pmod{n}$. If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0 - 1, n)$ gives a nontrivial factor of n. (Lemma)

Else, if $b_1 \equiv -1 \pmod{n}$, n is probably prime. (Can't apply Lemma) If $b_1 \not\equiv \pm 1 \pmod{n}$, set $b_2 \equiv b_1^2 \pmod{n}$.

If $b_2 \equiv 1 \pmod{n}$ then n is composite. If $b_2 \equiv -1 \pmod{n}$ then n is probably prime. Otherwise, set $b_3 \equiv b_2^2 \pmod{n}$.

Continue until stopping or reaching b_{k-1}. If $b_{k-1} \not\equiv -1 \pmod{n}$ and $k > 1$ then n is composite.

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$.

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$2^8 \equiv 256 \pmod{561}$$

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$2^8 \equiv 256 \pmod{561}$$
$$2^{16} \equiv 460 \pmod{561}$$

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \end{aligned}$$

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561} \end{aligned}$$

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561} \end{aligned}$$

We set $b_0 = 263$.

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561} \end{aligned}$$

We set $b_0 = 263$. Since $b_0 \not\equiv \pm 1 \pmod{561}$, we square to get $b_1 \equiv b_0^2 \equiv 166 \pmod{561}$.

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned}
2^8 &\equiv 256 \pmod{561} \\
2^{16} &\equiv 460 \pmod{561} \\
2^{32} &\equiv 103 \pmod{561} \\
2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561}
\end{aligned}$$

We set $b_0 = 263$. Since $b_0 \not\equiv \pm 1 \pmod{561}$, we square to get $b_1 \equiv b_0^2 \equiv 166 \pmod{561}$. Continuing:

$$b_1 \equiv 166 \pmod{561}$$

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561} \end{aligned}$$

We set $b_0 = 263$. Since $b_0 \not\equiv \pm 1 \pmod{561}$, we square to get $b_1 \equiv b_0^2 \equiv 166 \pmod{561}$. Continuing:

$$\begin{aligned} b_1 &\equiv 166 \pmod{561} \\ b_2 &\equiv 67 \pmod{561} \end{aligned}$$

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned}
2^8 &\equiv 256 \pmod{561} \\
2^{16} &\equiv 460 \pmod{561} \\
2^{32} &\equiv 103 \pmod{561} \\
2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561}
\end{aligned}$$

We set $b_0 = 263$. Since $b_0 \not\equiv \pm 1 \pmod{561}$, we square to get $b_1 \equiv b_0^2 \equiv 166 \pmod{561}$. Continuing:

$$\begin{aligned}
b_1 &\equiv 166 \pmod{561} \\
b_2 &\equiv 67 \pmod{561} \\
b_3 &\equiv 1 \pmod{561}.
\end{aligned}$$

Miller-Rabin Primality Test

Example

Let $n = 561$ and $a = 2$. Note $n - 1 = 560 = 2^4 \cdot 35$. Then

$$\begin{aligned} 2^8 &\equiv 256 \pmod{561} \\ 2^{16} &\equiv 460 \pmod{561} \\ 2^{32} &\equiv 103 \pmod{561} \\ 2^{35} &\equiv 8 \cdot 103 \equiv 263 \pmod{561} \end{aligned}$$

We set $b_0 = 263$. Since $b_0 \not\equiv \pm 1 \pmod{561}$, we square to get $b_1 \equiv b_0^2 \equiv 166 \pmod{561}$. Continuing:

$$\begin{aligned} b_1 &\equiv 166 \pmod{561} \\ b_2 &\equiv 67 \pmod{561} \\ b_3 &\equiv 1 \pmod{561}. \end{aligned}$$

So $\gcd(67 - 1, 561) = 33$ is a divisor of 561.

Pseudoprimes

Definition

An integer $n > 1$ that passes the Fermat Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a pseudoprime to base a.

Pseudoprimes

Definition

An integer $n > 1$ that passes the Fermat Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a pseudoprime to base a.

Definition

An integer $n > 1$ that passes the Miller-Rabin Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a strong pseudoprime to base a.

Pseudoprimes

Definition

An integer $n > 1$ that passes the Fermat Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a pseudoprime to base a.

Definition

An integer $n > 1$ that passes the Miller-Rabin Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a strong pseudoprime to base a.

Example

We saw that 561 was a pseudoprime to base 2 but not a strong pseudoprime to base 2.

Pseudoprimes

Definition

An integer $n > 1$ that passes the Fermat Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a pseudoprime to base a.

Definition

An integer $n > 1$ that passes the Miller-Rabin Primality Test using a base $a \in \mathbb{Z}$ for exponentiation is called a strong pseudoprime to base a.

Example

We saw that 561 was a pseudoprime to base 2 but not a strong pseudoprime to base 2.

Example

4097 is a strong pseudoprime to base 8, but not to base 2 or 4.

Pseudoprimes

Fix an integer $n > 4$. Let

$$W_n = \{b : 1 < b < n, \text{and } n \text{ is a strong pseudoprime to base } b\}.$$

Rabin[1] proved that if n is composite, then $\#W_n \leq n/4$.

[1] *Probabalistic Algorithm for Testing Primality.* Journal of Number Theory **12**, 128–138 (1980)

Pseudoprimes

Fix an integer $n > 4$. Let

$$W_n = \{b : 1 < b < n, \text{and } n \text{ is a strong pseudoprime to base } b\}.$$

Rabin[1] proved that if n is composite, then $\#W_n \leq n/4$.

Corollary

Let $n > 4$ be a composite integer.

Assume that the integers $b \in W_n$ are randomly and uniformly distributed among $(1, n)$. Let $a \in (1, n)$ be a random integer.

Then the Miller-Rabin Primality Test for a falsely claims that n is prime with probability at most $1/4$.

---

[1] *Probabalistic Algorithm for Testing Primality.* Journal of Number Theory **12**, 128–138 (1980)

Pseudoprimes

Fix an integer $n > 4$. Let

$$W_n = \{b : 1 < b < n, \text{and } n \text{ is a strong pseudoprime to base } b\}.$$

Rabin[1] proved that if n is composite, then $\#W_n \leq n/4$.

Corollary

Let $n > 4$ be a composite integer.

Assume that the integers $b \in W_n$ are randomly and uniformly distributed among $(1, n)$. Let $a_1, \ldots, a_k \in (1, n)$ be k randomly selected integers.

Then the Miller-Rabin Primality Test for $a_1, \ldots, a_k$ falsely claims that n is prime with probability at most $(1/4)^k$.

[1] *Probabalistic Algorithm for Testing Primality.* Journal of Number Theory **12**, 128–138 (1980)

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

- Bob first needs to choose large primes $p \neq q$.

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

- Bob first needs to choose large primes $p \neq q$.
- To do this, Bob can randomly select a starting integer m of the appropriate size.

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

- Bob first needs to choose large primes $p \neq q$.
- To do this, Bob can randomly select a starting integer m of the appropriate size.
- Bob can then use the Miller-Rabin Test to verify whether m is composite. If m is confirmed to be composite, then Bob should continue his search.

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

- Bob first needs to choose large primes $p \neq q$.
- To do this, Bob can randomly select a starting integer m of the appropriate size.
- Bob can then use the Miller-Rabin Test to verify whether m is composite. If m is confirmed to be composite, then Bob should continue his search.
- If m is not confirmed to be composite, then Bob can run the Miller-Rabin Primality Test k times to gain assurance that, if m is composite, then m is composite with probability less than $(1/4)^k$.

Primes for RSA

Bob wants to implement an RSA encryption-decryption scheme.

- Bob first needs to choose large primes $p \neq q$.
- To do this, Bob can randomly select a starting integer m of the appropriate size.
- Bob can then use the Miller-Rabin Test to verify whether m is composite. If m is confirmed to be composite, then Bob should continue his search.
- If m is not confirmed to be composite, then Bob can run the Miller-Rabin Primality Test k times to gain assurance that, if m is composite, then m is composite with probability less than $(1/4)^k$.
- Bob continues until he finds an integer m which passes all k tests. Bob can then set $p = m$.

Cautions

Choosing q given p

Bob is implementing an RSA encryption-decryption scheme. He has found one prime p.

[2] *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* Journal of Cryptology, **10**, 233–260 (1997)

Choosing q given p

Bob is implementing an RSA encryption-decryption scheme. He has found one prime p.

- Bob shouldn't pick q to be the next prime larger than p.

[2] *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* Journal of Cryptology, **10**, 233–260 (1997)

Choosing q given p

Bob is implementing an RSA encryption-decryption scheme. He has found one prime p.

- Bob shouldn't pick q to be the next prime larger than p. If he did, then a brute force attack of trial division starting from the smallest integer at least $\sqrt{n}$ would factor n quickly.

[2] *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* Journal of Cryptology, **10**, 233–260 (1997)

Choosing q given p

Bob is implementing an RSA encryption-decryption scheme. He has found one prime p.

- Bob shouldn't pick q to be the next prime larger than p. If he did, then a brute force attack of trial division starting from the smallest integer at least $\sqrt{n}$ would factor n quickly.
- Bob should try to avoid adding too many predictable digits to q. (E.g. testing the integers $p \cdot 10^{150} + k$ for increasing $k \geq 1$).

[2] *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* Journal of Cryptology, **10**, 233–260 (1997)

Choosing q given p

Bob is implementing an RSA encryption-decryption scheme. He has found one prime p.

- Bob shouldn't pick q to be the next prime larger than p. If he did, then a brute force attack of trial division starting from the smallest integer at least $\sqrt{n}$ would factor n quickly.
- Bob should try to avoid adding too many predictable digits to q. (E.g. testing the integers $p \cdot 10^{150} + k$ for increasing $k \geq 1$).

Theorem (Coppersmith[2])

Let $n = pq$ have d digits. Then, given either the first $d/4$ or the last $d/4$ digits of q, there is an efficient algorithm for factoring n.

[2] *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* Journal of Cryptology, **10**, 233–260 (1997)

Choosing q given p

Care should be taken in how one “randomly” generates p and q.

Choosing q given p

Care should be taken in how one “randomly” generates p and q.

In 2012, Arjen Lenstra and others collected 11.4×10^6 public moduli n used for RSA encryption. They computed the pairwise gcd of these moduli and found that 26965 where the gcd gave a nontrivial factor.

Choosing q given p

Care should be taken in how one "randomly" generates p and q.

In 2012, Arjen Lenstra and others collected 11.4×10^6 public moduli n used for RSA encryption. They computed the pairwise gcd of these moduli and found that 26965 where the gcd gave a nontrivial factor.

The probability of finding a pair when choosing r items from N (allowing repetition in choice) is

$$\mathbb{P}(r \text{ from } n) \approx 1 - e^{-r^2/2N}$$

when N is large.

Choosing q given p

Care should be taken in how one “randomly” generates p and q.

In 2012, Arjen Lenstra and others collected 11.4×10^6 public moduli n used for RSA encryption. They computed the pairwise gcd of these moduli and found that 26965 where the gcd gave a nontrivial factor.

The probability of finding a pair when choosing r items from N (allowing repetition in choice) is

$$\mathbb{P}(r \text{ from } n) \approx 1 - e^{-r^2/2N}$$

when N is large.

Consider when N is the collection of possible primes that any RSA program can produce, and r is the number of RSA moduli used.