RSA III

Primality tests & primality proofs

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

How to pick p and q in RSA KeyGen?

1. Generate p:
   1.1 Pick random odd number of $\ell/2$ bits.
   1.2 If number is prime, output, else return to 1.1.
2. Generate q
   2.1 Pick random odd number of $\ell/2$ bits.
   2.2 If number is prime, output, else return to 2.1.
3. Relabel to have $p < q$.

How do we find out "If number is prime"?

How to pick p and q in RSA KeyGen?

1. Generate p:
   1.1 Pick random odd number of $\ell/2$ bits.
   1.2 If number is prime, output, else return to 1.1.
2. Generate q
   2.1 Pick random odd number of $\ell/2$ bits.
   2.2 If number is prime, output, else return to 2.1.
3. Relabel to have $p < q$.

How do we find out "If number is prime"?
Could try trial division up to $\sqrt{p}$ / sieve of Eratosthenes.

How to pick p and q in RSA KeyGen?

1. Generate p:
   1.1 Pick random odd number of $\ell/2$ bits.
   1.2 If number is prime, output, else return to 1.1.
2. Generate q
   2.1 Pick random odd number of $\ell/2$ bits.
   2.2 If number is prime, output, else return to 2.1.
3. Relabel to have $p < q$.

How do we find out "If number is prime"?
Could try trial division up to $\sqrt{p}$ / sieve of Eratosthenes.
Numbers within reach would be easy to factor by the same methods.

Primality tests and primality proofs work much faster but do not (typically) find factors of composite numbers.

How to pick p and q in RSA KeyGen?

1. Generate p:
   1.1 Pick random odd number of $\ell/2$ bits.
   1.2 If number is prime, output, else return to 1.1.
2. Generate q
   2.1 Pick random odd number of $\ell/2$ bits.
   2.2 If number is prime, output, else return to 2.1.
3. Relabel to have $p < q$.

How do we find out "If number is prime"?
Could try trial division up to $\sqrt{p}$ / sieve of Eratosthenes.
Numbers within reach would be easy to factor by the same methods.

Primality tests and primality proofs work much faster but do not (typically) find factors of composite numbers.

A primality test is correct if it outputs "composite", does not give definitive answer on primality. (Better called compositeness proofs).

A primality proof is correct if it outputs "prime", does not give definitive answer on compositeness.

Fermat's primality test

If p is prime then
$$a^{p-1} \equiv 1 \bmod p$$
for all $0 < a < p$.

Fermat's primality test

If p is prime then

$$a^{p-1} \equiv 1 \bmod p$$

for all $0 < a < p$.

Fermat's primality test repeats the following steps with different choices of $1 < a < p$:

1. If $\gcd(a, p) \neq 1$ output "composite, factor $\gcd(a, p)$".
2. If $a^{p-1} \not\equiv 1 \bmod p$ output "composite".
3. Else output "probably prime".

Most composite numbers get caught after a few runs of Fermat's primality test.

Fermat's primality test

If p is prime then
$$a^{p-1} \equiv 1 \bmod p$$
for all $0 < a < p$.

Fermat's primality test repeats the following steps with different choices of $1 < a < p$:

1. If $\gcd(a, p) \neq 1$ output "composite, factor $\gcd(a, p)$".
2. If $a^{p-1} \not\equiv 1 \bmod p$ output "composite".
3. Else output "probably prime".

Most composite numbers get caught after a few runs of Fermat's primality test.

Carmichael numbers are a class of exceptions to Fermat's primality test.
These are composite numbers m so that $a^{n-1} \equiv 1 \bmod n$ for all $0 < a < n$ with $\gcd(a, n) = 1$.
These still get caught in the first step, but take a lot longer to find.

Miller–Rabin primality test

This test does not have exceptions.

If p is prime then $a^2 \equiv 1 \bmod p$ has exactly 2 solutions $a \equiv \pm 1 \bmod p$.

If $n = pq$ for primes p, q then

$$\begin{aligned} a &\equiv 1 \bmod p \\ a &\equiv -1 \bmod q \end{aligned}$$

describes $a \not\equiv \pm 1 \bmod n$ with $a^2 \equiv 1 \bmod n$ by CRT.

Example: $4^2 \equiv 1 \bmod 15$ and $4 \equiv 1 \bmod 3, 4 \equiv -1 \bmod 5$..

For a composite n at most $1/2$ of a with $a^2 \equiv 1 \bmod n$ are in ± 1.

Miller–Rabin primality test

This test does not have exceptions.

If p is prime then $a^2 \equiv 1 \bmod p$ has exactly 2 solutions $a \equiv \pm 1 \bmod p$.

If $n = pq$ for primes p, q then

$$\begin{aligned} a &\equiv 1 \bmod p \\ a &\equiv -1 \bmod q \end{aligned}$$

describes $a \not\equiv \pm 1 \bmod n$ with $a^2 \equiv 1 \bmod n$ by CRT.

Example: $4^2 \equiv 1 \bmod 15$ and $4 \equiv 1 \bmod 3, 4 \equiv -1 \bmod 5$..

For a composite n at most $1/2$ of a with $a^2 \equiv 1 \bmod n$ are in ± 1.

Problem: we cannot compute square roots.

Miller–Rabin primality test

This test does not have exceptions.

If p is prime then $a^2 \equiv 1 \bmod p$ has exactly 2 solutions $a \equiv \pm 1 \bmod p$.

If $n = pq$ for primes p, q then

$$\begin{aligned} a &\equiv 1 \bmod p \\ a &\equiv -1 \bmod q \end{aligned}$$

describes $a \not\equiv \pm 1 \bmod n$ with $a^2 \equiv 1 \bmod n$ by CRT.

Example: $4^2 \equiv 1 \bmod 15$ and $4 \equiv 1 \bmod 3, 4 \equiv -1 \bmod 5$..

For a composite n at most $1/2$ of a with $a^2 \equiv 1 \bmod n$ are in ± 1.

Problem: we cannot compute square roots.

Can compute exponentiation with integer exponent.
For p a prime, $a^{(p-1)/2} \equiv \pm 1 \bmod p$ because of Fermat.
If this is 1 try $a^{(p-1)/4}$ etc. – provided that $p - 1$ is divisible by 4, 8 etc.

Miller–Rabin primality test

This test does not have exceptions.

If p is prime then $a^2 \equiv 1 \bmod p$ has exactly 2 solutions $a \equiv \pm 1 \bmod p$.

If $n = pq$ for primes p, q then

$$\begin{aligned} a &\equiv 1 \bmod p \\ a &\equiv -1 \bmod q \end{aligned}$$

describes $a \not\equiv \pm 1 \bmod n$ with $a^2 \equiv 1 \bmod n$ by CRT.

Example: $4^2 \equiv 1 \bmod 15$ and $4 \equiv 1 \bmod 3, 4 \equiv -1 \bmod 5$..

For a composite n at most $1/2$ of a with $a^2 \equiv 1 \bmod n$ are in ± 1.

Problem: we cannot compute square roots.

Can compute exponentiation with integer exponent.
For p a prime, $a^{(p-1)/2} \equiv \pm 1 \bmod p$ because of Fermat.
If this is 1 try $a^{(p-1)/4}$ etc. – provided that $p - 1$ is divisible by 4, 8 etc.

Let $p - 1 = 2^s t$ with t odd. So we can compute $a^{(p-1)/2^s}$.

Miller–Rabin primality test

Let $p-1 = 2^s t$ with t odd.

1. Pick random $1 < b < p$.
2. Compute $c \equiv b^t \bmod p$.
3. If $c \equiv \pm 1 \bmod p$ output "probably prime".
4. For $i = 1$ to $s-1$
   4.1 $c \leftarrow c^2 \bmod p$.
   4.2 If $c = 1$ output "composite".
   4.3 If $c = -1$ output "probably prime"
5. Output "composite".

c will square to 1, so no info.

$\leftarrow$ means to assign

p does not pass Fermat test or $c \neq \pm 1$ squares to 1.

Miller–Rabin primality test

Let $p-1=2^st$ with t odd.

1. Pick random $1<b<p$.
2. Compute $c\equiv b^t \bmod p$.
3. If $c\equiv \pm 1 \bmod p$ output "probably prime".
4. For $i=1$ to $s-1$
   4.1 $c \leftarrow c^2 \bmod p$.
   4.2 If $c=1$ output "composite".
   4.3 If $c=-1$ output "probably prime"
5. Output "composite".

c will square to 1, so no info.

$\leftarrow$ means to assign

p does not pass Fermat test
or $c\neq \pm 1$ squares to 1.

Composite p has probability $\leq 1/2$ of passing as "probably prime".

Repeat k times to probability $\leq 1/2^k$ of passing as "probably prime".

Pocklington primality proof

This criterion fails for some p.

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

Else p fails Fermat test for a.

Else we get a factor of p.

Pocklington primality proof

This criterion fails for some p.

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

Else p fails Fermat test for a.

Else we get a factor of p.

Example:
$p = 103$, so $p - 1 = 102 = 2 \cdot 3 \cdot 17$.
Put $q = 17$ then $q > \sqrt{103} - 1 = 9.148\ldots$.

Pocklington primality proof

This criterion fails for some p.

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

Else p fails Fermat test for a.

Else we get a factor of p.

Example:
$p = 103$, so $p - 1 = 102 = 2 \cdot 3 \cdot 17$.
Put $q = 17$ then $q > \sqrt{103} - 1 = 9.148\ldots$.

Take $a = 2$. Compute $2^{102} \equiv 1 \bmod 103$.
$\gcd(2^{(103-1)/17} - 1, 103) = \gcd(2^6 - 1, 103) = \gcd(63, 103) = 1$.

Pocklington primality proof

This criterion fails for some p.

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

Else p fails Fermat test for a.

Else we get a factor of p.

Example:
$p = 103$, so $p - 1 = 102 = 2 \cdot 3 \cdot 17$.
Put $q = 17$ then $q > \sqrt{103} - 1 = 9.148\ldots$.

Take $a = 2$. Compute $2^{102} \equiv 1 \bmod 103$.
$\gcd(2^{(103-1)/17} - 1, 103) = \gcd(2^6 - 1, 103) = \gcd(63, 103) = 1$.

This shows that 103 is prime if 17 is prime.

Pocklington primality proof

This criterion fails for some p.

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

Else p fails Fermat test for a.

Else we get a factor of p.

Example:
$p = 103$, so $p - 1 = 102 = 2 \cdot 3 \cdot 17$.
Put $q = 17$ then $q > \sqrt{103} - 1 = 9.148\ldots$.
Take $a = 2$. Compute $2^{102} \equiv 1 \bmod 103$.
$\gcd(2^{(103-1)/17} - 1, 103) = \gcd(2^6 - 1, 103) = \gcd(63, 103) = 1$.

This shows that 103 is prime if 17 is prime.

Because $17 - 1 = 2^4$ we cannot use Pocklington to prove primality.
But this is a smaller problem (still more than half the bitlength).

Pocklington primality proof

If there exist $a, q \in \mathbf{N}$ with

- q prime, $q|(p-1)$, and $q > \sqrt{p} - 1$,
- $a^{p-1} \equiv 1 \bmod p$, and
- $\gcd(a^{(p-1)/q} - 1, p) = 1$ then p is prime.

This criterion fails for some p.

Else p fails Fermat test for a.

Else we get a factor of p.

Example:
$p = 103$, so $p - 1 = 102 = 2 \cdot 3 \cdot 17$.
Put $q = 17$ then $q > \sqrt{103} - 1 = 9.148\ldots$.

Take $a = 2$. Compute $2^{102} \equiv 1 \bmod 103$.
$\gcd(2^{(103-1)/17} - 1, 103) = \gcd(2^6 - 1, 103) = \gcd(63, 103) = 1$.

This shows that 103 is prime if 17 is prime.

Because $17 - 1 = 2^4$ we cannot use Pocklington to prove primality.
But this is a smaller problem (still more than half the bitlength).

Pocklington leads to sequence of primes, here 103, 17.
Generalizations exist.
Much more general ECPP: elliptic-curve primality proofs.