Tyler Hardman
John Martinez
MATH 4513
26-4-06

What is RSA and what are some algorithms that make attempts at cracking it?

Simply put, RSA is an encryption algorithm developed by Rivest, Shamir and Adleman at MIT in 1971.

Encryption

Basic premise: sending a message that only the sender and the recipient are able to read.

Step 1: Convert the message into an integer a, called the plaintext.

Step 2: Apply the encryption function $E(x)$ to get $E(a) = b$, called the cryptogram. The cryptogram is the thing that is sent.

Step 3: Apply the decryption function $D(x)$ to get $D(b) = a$.

So, we have

$$\text{plaintext} \xrightarrow{E} \text{cryptogram} \xrightarrow{D} \text{plaintext}$$

Note that E and D must be 1-1, otherwise the received plaintext would be ambiguous.

Note that $D(E(a)) = a$, so D is the inverse of E.

RSA

Defn Let n be a positive integer. Then $\phi(n)$ denotes the number of integers $< n$ that are relatively prime to n, including 1.

Now, to find E and D:

Let p and q be large primes.

Let $n = p \cdot q$.

Proposition If $n = p \cdot q$ where p, q prime then $\phi(n) = (p-1)(q-1)$

Note: this is not a rigorous proof!

Proof: There are $n-1$ integers less than n. Thus, $\phi(n)$ is just $(n-1)$ minus the number of integers that aren't relatively prime to n. Let this number be denoted by $\bar{\phi}(n)$.

Because $n = p \cdot q$, if a is not relatively prime to n, then $a = kp$ or $a = lq$, where $0 < k < q-1$ and $0 < l < p-1$.

Thus there are $q-1$ multiples of p less than n and there are $p-1$ multiples of q less than n, so $\bar{\phi}(n) = q-1+p-1$.

Then $$\begin{aligned}\phi(n) &= (n-1) - \bar{\phi}(n) \\ &= n-1-(p+q-2) \\ &= pq-p-q+1 \\ &= (p-1)(q-1)\end{aligned}$$

Now let e be a small prime number such that $GCD(e, \phi(n)) = 1$.

Then, for plaintext a, $0 \le a < n$,

$E(a) = a^e \bmod n = b$.

Now find d s.t. $de \equiv 1 \pmod{\phi(n)}$.

Then for cryptogram b,

$D(b) = b^d \bmod n = a$.

Proof that the algorithm works

Theorem (Fermat)

Let $p > 0$ be a prime number and a be an integer.

Then $a^p \equiv a \pmod p$

Proof (by induction)

Let $a = 1$. Then $a^p = 1^p = 1 = a$

$\Rightarrow a^p \equiv a \pmod p$

Now suppose $n^p \equiv n \pmod p$

By a corollary to the Binomial Theorem,

$(a+b)^p \equiv a^p + b^p \pmod p$

Then $(n+1)^p \equiv n^p + 1^p \pmod p$

$\equiv n^p + 1 \pmod p$

$\equiv n+1 \pmod p$

$\blacksquare$

Now, to show that $D(E(a)) = a$:

$E(a) = a^e \bmod n$

$D(E(a)) \equiv (a^e)^d \pmod n$

$\equiv a^{ed} \pmod n$

By definition, $de \equiv 1 \pmod{\phi(n)}$

$\Rightarrow \exists k$ s.t. $de = 1 + k\phi(n) = 1 + k(p-1)(q-1)$

Then

$$a^{ed} = a^{1+k(p-1)(q-1)}$$
$$= a(a^{p-1})^{k(q-1)}$$

and thus

$$a^{ed} \equiv a(a^{p-1})^{k(q-1)} \pmod p$$

Case 1: if p divides a, then

$a^{ed} \equiv 0 \pmod p$ and $a \equiv 0 \pmod p$

Therefore $a^{ed} \equiv a \pmod p$

Case 2: if p does not divide a, then

$a^{ed} \equiv a(a^{p-1})^{k(q-1)} \pmod p$

By Fermat's Theorem,

$a^p \equiv a \pmod p$

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

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

$a^{ed} \equiv a(1)^{k(q-1)} \pmod p$

$\equiv a \pmod p$

The same argument can be used to show that

$a^{ed} \equiv a \pmod q$

Thus $a^{ed} - a \equiv 0 \pmod p$ and $a^{ed} - a \equiv 0 \pmod q$

$p \mid a^{ed} - a$ and $q \mid a^{ed} - a$

Using part (2) of the provided lemma:

If a and b divide c, then ab divides c.

Thus

$$pq \mid a^{ed} - a$$

$$n \mid a^{ed} - a$$

$$a^{ed} - a \equiv 0 \pmod{n}$$

$$a^{ed} \equiv a \pmod{n}$$

$$D(E(a)) \equiv a \pmod{n}$$

Because $0 \leq a < n$ and, by definition, $0 \leq D(E(a)) < n$, we have

$$D(E(a)) = a$$

$\blacksquare$

A brief example

Let $n = 55$, $e = 23$. Let our secret message will be 2 (for simplicity). To encode 2 perform $E = M^e \bmod n = 2^{23} \bmod 55 = 8$. So 8 is the encoded message and $e = 23$. I send publicly $(23, 8)$. The receiver obtains $(23, 8)$ and since they know the factorization of n they know $\phi(n)$, which in this case is $\phi(55) = 40$. So the receiver computes $e \cdot d \equiv 1 \bmod \phi(n) = 23 \cdot d \equiv 1 \bmod 40$. Adding $0 \equiv 160 \bmod 40$ to the congruence yields $23d \equiv 161 \bmod 40$. $\Rightarrow$ $d = 7 \bmod 40$ so $d = 7$. To decode the message, we take $8^7 \bmod 55 = 2$, our original message.

EFFORTS TO FACTOR $N = PQ$

In theory, factoring is easy. Simply take $\sqrt{n}$ and use trial division from 2 up to $\sqrt{n}$. Given an $n = pq$ such as $55 = 5 \cdot 11$, this trial division is easy and can be done in a short amount of time. However consider an RSA moduli of 1×10^{200}. Then $\sqrt{1 \times 10^{200}} = 1 \times 10^{100}$. So if a computer could check every prime less Than 1×10^{100} in a second, it would take 1.4×10^{90} years, since there are $\pi(1 \times 10^{100}) \sim Li(1 \times 10^{100}) \approx 4.4 \times 10^{97}$ prime less Than 1×10^{100}. This is absurd and is impossible to compute. So then must be better ways.

Fermat's Algorithm

let $n = pq$; $p > q$. Then $x = \frac{p+q}{2}$ and $y = \frac{p-q}{2}$,

then $x^2 - y^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = \frac{p^2+2pq+q^2-p^2+2pq-q^2}{4} = pq = n$

then set $x = \lceil \sqrt{n} \rceil$ and $y = 1$. increase y by 1 until $x^2 - y^2 \leq n$ if it is strictly equal, factorization is complete, if not increase x by one and start with $y=1$ again and increment y by 1 until $x^2 - y^2 \leq n$. repeat this until $x^2 - y^2 = n$.

b- Algorithm

define $z = \lfloor \sqrt{n} \rfloor$, $a = \lfloor n/z \rfloor \geq z$ and $n - az = r$.
if $n = pq$ with $p > q$, then we can write $q = a - x$ for some $x \in \mathbb{Z}^+$. so $n = (a-x)\left(z + \frac{zx+r}{a-x}\right)$

proof.

$$n = p \cdot q = (a-x)_1 = (a-x)(z+p-z) = (a-x)\left(z + \frac{n-zq}{q}\right) =$$

$$(a-x)\left(z + \frac{az+r-z(a-x)}{a-x}\right) = (a-x)\left(z + \frac{zx+r}{a-x}\right) \blacksquare \quad \text{So}$$

$$n = (a-x)\left(z + f(x)\right) \; ; \quad f(x) = \frac{zx+r}{a-x} = p - z \in \mathbb{Z}.$$

also, $p = a - x'$ where $x' \in \mathbb{Z}^-$ which yields $q = z + f(x')$

so $$\frac{f(x) - f(x')}{x - x'} = \frac{(p-z) - (q-z)}{(a-q) - (a-p)} = \frac{p-q}{p-q} = 1$$

So $(x, f(x))$, $(x', F(x'))$ are points with slope 1. and a y intercept at b.

Then $x+b = \dfrac{2x+r}{a-x}$ or $x^2 + x(2-a+b)+r-ab=0$

by the quadratic formula

$$x = \frac{a-2-b+\sqrt{(2-a+b)^2-4(r-ab)}}{2}$$. so once

we find b, n is factored.

example $n = 4141$ $z = \lfloor\sqrt{4141}\rfloor = 64$ $\lfloor 4141/64 \rfloor = 64$

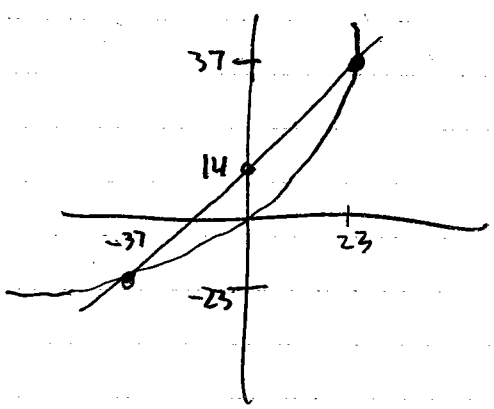
$4141 - 64^2 = 45$ so

$f(x) = \dfrac{64x+45}{64-x}$. The quadratic eq. gives

$$x = \frac{-b \pm \sqrt{b^2-4(45-64b)}}{2}$$ with $b = 2, 4, \ldots, 2n$.

at $b=14$ we obtain $\dfrac{-14 \pm \sqrt{14^2-4(45-64\cdot 14)}}{2} = \dfrac{-14 \pm 60}{2} = 23, -37$

So $64-23 = 41$ and $64-(-37) = 101$. so n is factored.



Bibliography

[1] Coutinho, S. C. The Mathematics of Ciphers.
Copyright © 1999 A K Peters, Ltd.

[2] Riesel, Hans. Prime Numbers & Computer Methods for Factorization. Edited by J. Coates & S. Helgason
Copyright © 1985 by Birkhäuser Boston, Inc.

[3] Lucarelli, Vincent. On Factoring n with the b-algorithm
"The College Journal of Mathematics" Vol. 29, No. 4
September 1998. pg. 289 - 295.

Fermat's theorem. *Let $p > 0$ be a prime number and let a be an integer; then*

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

To prove this theorem using finite induction we must find a proposition $P(n)$ to which the method can be applied. The proposition is

$$n^p \equiv n \pmod{p} \quad \text{for an integer} \quad n.$$

Note that the proposition says only that the congruence of the theorem holds for positive integers. Thus, apparently, we are not proving the theorem in full generality. However, every integer is congruent, modulo p, to a non-negative integer smaller than p. Hence, it is enough to prove the theorem for $0 \leq a \leq p-1$. In particular, the theorem follows if we prove that the proposition $P(n)$ holds for every $n \geq 1$.

Of course $P(1)$ holds, since $1^p = 1$. To go from $P(n)$ to $P(n+1)$ we must find a way to relate these two statements. This is provided by the *binomial theorem*. The proof becomes considerably simpler if we isolate as an auxiliary result what is really a version of the binomial theorem for integers modulo p.

Lemma. *Let $p > 0$ be a prime number and let a and b be integers; then*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Proof of the lemma. It follows from the binomial formula that

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i.$$

Thus, to prove the lemma, it is enough to show that

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i \equiv 0 \pmod{p}.$$

But this follows immediately if we prove that the binomial numbers $\binom{p}{i}$ are divisible by p for $1 \leq i \leq p-1$. Now, by definition

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}.$$

Since binomial numbers are integers, the denominator of this fraction must divide the numerator. But if $1 \leq i \leq p-1$, then p is *not* a factor of $i!$ Thus the factor p that appears in the numerator of the fraction will *not* be canceled by the denominator. Therefore $i!$ must divide $(p-1)\ldots(p-i+1)$ and we have that $\binom{p}{i}$ is a multiple of p, as we wanted to prove.

We may now return to the proof of Fermat's theorem. The induction hypothesis is

$$n^p \equiv n \pmod{p} \quad \text{for some integer} \quad n,$$

and we must show that $(n+1)^p \equiv n+1 \pmod{p}$. By the lemma

$$(n+1)^p \equiv n^p + 1^p \equiv n^p + 1 \pmod{p}.$$

By the induction hypothesis we can replace n^p by n in this formula. Doing this, we conclude that

$$(n+1)^p \equiv n^p + 1 \equiv n+1 \pmod{p},$$

as we wanted to prove.

Lemma. *Let a, b, and c be positive integers, and assume that a and b are co-prime.*

(1) *If b divides the product ac, then b divides c.*
(2) *If a and b divide c, then the product ab divides c.*

Let's prove (1) first. We have, by hypothesis, that a and b are co-prime; that is, $\gcd(a, b) = 1$. It follows by the extended Euclidean algorithm that there exist integers α and β such that

$$\alpha a + \beta b = 1.$$

Now we come to the "abracadabra" of this proof: Multiply both sides of the equation by c. This gives

$$\alpha ac + \beta cb = c. \tag{6.1}$$

The second term on the left-hand side is clearly divisible by b, but so is the first term. Indeed, it is divisible by ac, which is a multiple of b, by hypothesis. Thus the left-hand side of (6.1) is itself a multiple of b. Since it is equal to c, we have proved (1).

Now we use (1) to prove (2). If a divides c, then there exists an integer t such that $c = at$. But b also divides c. Since a and b are co-prime, it follows from (1) and $c = at$ that b must divide t. Thus $t = bk$ for some integer k. Hence

$$c = at = a(bk) = (ab)k$$

is divisible by ab, which is the conclusion of (2).