RSA

MATH 195

Algebraic Setup

We begin with a theorem from group theory:

Theorem (Lagrange)**.** *If G is a finite group, $\#G = n < \infty$, then for all $g \in G$, one has $g^n = e$.*

Quick proof, G abelian. Fix $g \in G$, then $G \to G$ by $x \mapsto gx$ is bijective (the map $x \mapsto g^{-1}x$ is its inverse. Hence

$$\prod_{y \in G} y = \prod_{x \in G} (gx) = g^n \prod_{x \in G} x$$

so $e = g^n$. ☐

Special case: Let k be a finite field, $\#k = q$. Then for all $\alpha \in k^*$, $\alpha^{q-1} = 1$. Apply Lagrange's theorem to $G = k^* = k \setminus \{0\}$. Including $\alpha = 0$, we have for all $\alpha \in k$, $\alpha^q = \alpha$.

Example. If $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for p prime, then $a^p = a$ for all $a \in \mathbb{Z}/p\mathbb{Z}$, in other words, we have the (little) theorem of Fermat: for all integers $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$ for p prime.

Notice that for all $a \in (\mathbb{Z}/p\mathbb{Z})^*$, $a^{p-1} = 1$, $a^{2(p-1)} = 1$, and so on, so that $a^\ell = 1$ if $\ell \equiv 0 \pmod{p-1}$. Then for all $a \in \mathbb{Z}$, and all $m \in \mathbb{Z}_{\geq 0}$ such that $m \equiv 1 \pmod{p-1}$, $a^m \equiv a \pmod{p}$.

Proposition. *Let p and q be two prime numbers, $p \neq q$, and put $n = pq$. Then for all positive integers $m \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$ and all $a \in \mathbb{Z}/n\mathbb{Z}$, one has $a^m = a$ (in $\mathbb{Z}/n\mathbb{Z}$), which is to say*

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

for all integers a.

Recall that the *least common multiple* of integers k and ℓ is the smallest positive integer divisible both by k and by ℓ. For example, $\operatorname{lcm}(12, 18) = 36$. Note that $\operatorname{lcm}(k, \ell) = k\ell/\gcd(k, \ell)$. Note then that if $m \equiv 1 \pmod{(p-1)(q-1)}$, then $m \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$.

This proposition is the backbone of the RSA cryptosystem.

Proof. Take $a \in \mathbb{Z}$. Then $m \equiv 1 \pmod{p-1}$, since $\operatorname{lcm}(p-1, q-1) \mid (m-1)$ but by definition $(p-1) \mid \operatorname{lcm}(p-1, q-1)$. So by Fermat's little theorem, $a^m \equiv a \pmod{p}$ which is to say $p \mid (a^m - a)$. The same is true for q, so $q \mid (a^m - a)$. Hence

This is some of the material covered February 26, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight jvoight@math.berkeley.edu.

$n = pq \mid (a^m - a)$, since it is divisible by these distinct primes, and hence $a^m \equiv a \pmod{n}$. □

Remark. We can get this from Lagrange's theorem. We take $G = (\mathbb{Z}/n\mathbb{Z})^*$. We have

$$\#G = \phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Therefore for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. But this only gives us the statement for the product $(p-1)(q-1)$, and only for elements $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Example. Take $p = 5$, $q = 7$, and $\mathrm{lcm}(p-1, q-1) = \mathrm{lcm}(4,6) = 12$. Take $m = 13 \equiv 1 \pmod{12}$, and $a = 2$, then $2^{13} \equiv 2 \pmod{35}$, hence $5 \cdot 7 \mid 8190 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

Note that for all $m \equiv 1 \pmod{p-1}$, $2^m \equiv 2 \pmod{p}$, so $2^{13} \equiv 2 \pmod{p}$ for every prime p for which $(p-1) \mid 12$, i.e. $p - 1 = 1, 2, 3, 4, 6, 12$, or $p = 2, 3, 4, 5, 7, 13$, but 4 is not prime, so we could have known already that $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \mid 8190$.

RSA Cryptosytem

Recall we have Alice sending a message to Bob, with Eve listening.

The RSA-system is a block cipher, $\mathcal{P} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z}$ for an integer $n = pq$, where n (the *modulus*) is known to everybody, but the prime factors p, q are known only to Bob. We need in practice p and q to be very large (over 100 digits, say). We take $\mathcal{K}$ to be the set of positive integers relatively prime to $\mathrm{lcm}(p-1, q-1)$. The *encryption key* $e \in \mathcal{K}$ is known to everyone, but the *decryption key* $d \in \mathcal{K}$ is known only to Bob. Then Alice encrypts:

$$E : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$$
$$E(a, e) = a^e \pmod{n}$$

Eve knows a^e, e, and n, but does not know a.

To decrypt, Bob

$$D : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$$
$$D(b, e) = b^d \pmod{n}$$

where $ed \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$.

Claim. For all a, e, $D(E(a,e), e) = a$, since

$$D(E(a,e), e) = D(a^e, e) = (a^e)^d = a^{de} \equiv a \pmod{n}$$

by the proposition.

Warning: Given $n = pq$, and a multiple of $\mathrm{lcm}(p-1, q-1)$, one can compute p and q. For example, in the special case that we are given $\phi(n) = (p-1)(q-1) = pq - p - q + 1$, we note that

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - (n + 1 - \phi(n))x + n.$$

is a polynomial which gives the values of p and q by the quadratic formula. Therefore the secrets are in some sense equivalent: knowing p, q is equivalent to knowing $\phi(n)$, and vice versa.

Why is prime factorization a difficult problem? Only a historical one: it is an age-old problem, for centuries people have been thinking about it, but no fast methods have been arrived upon.