RSA Encryption

Fermat's Little Theorem

- If p is a prime number and a is an integer such that gcd(a,p) = 1, then $a^{p-1} = 1 \pmod p$
- Proof:
  - Consider the numbers (a, 2a, 3a, ..., (p-1)a), all mod p. They are all different. If any were the same, say Ma = Na (mod p), then (M-N)a = 0 (mod p), so M-N must be a multiple of p. But since M < p and N < p, M=N.
  - Thus, (a, 2a, 3a, ... (p-1)a) must be a rearrangement of (1, 2, 3, ... (p-1)). So, mod p, we have:

    $$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} ia = a^{p-1}\prod_{i=1}^{p-1} i$$

  - so $a^{p-1} = 1 \pmod p$

Chinese Remainder Theorem

- Let p and q be two integers such that gcd(p,q) = 1. If a = b (mod p) and a = b (mod q) then a = b (mod pq).
- Proof:
  - If a = b (mod p) then p divides (a - b). Similarly q divides (a - b). But, p and q are relatively prime, so pq divides (a - b). Consequently a = b (mod pq).

RSA Public Key Encryption

- Bob needs to send Alice a private communication.
- Bob looks up Alice's public key and encodes the message using it. Anyone can do this.
- Only Alice's private key can decode messages encoded in Alice's public key. Privacy is achieved.
- Bob encodes his signature on the message using Bob's private key.
- Alice decodes Bob's signature using Bob's public key. Anyone can do this. Authentication is achieved.
- Problem: What pair of functions are inverses of each other, but knowing one does not lead to figuring out the other?

RSA in Action

- Preparation:
  - Choose two large prime numbers, p and q
  - Compute $N = pq$
  - Choose a small integer relatively prime to $(p-1)(q-1)$, say e
  - Compute the multiplicative inverse of e, say d, (mod $(p-1)(q-1)$). That is, $ed = 1 \pmod{(p-1)(q-1)}$
  - Destroy p and q, publish (e,N) = public key, keep d private.
- Encoding a message M into a coded message C:
  - $C = M^e \pmod{N}$
- Decoding:
  - $M = C^d \pmod{N}$
- Knowing e and N, the only way to find d is to determine the modulus in which they are inverses, i.e. $(p-1)(q-1)$.
- The only way to know the modulus is to factor N into the primes p and q – an exponential problem.

Why does it work?

- Let p and q be two different large primes
- Let $0 \leq M \leq pq$ be the message
- Let d and e be two numbers such that $de = 1 \pmod{(p-1)(q-1)}$
- Let the encoded message $C = M^d \pmod{pq}$
- Prove $M = C^e \pmod{pq}$
  - $de = 1 \pmod{(p-1)(q-1)} \Rightarrow de = 1 + k(p-1)(q-1)$ for some integer k
  - $C^e = M^{de} = M^{1+k(p-1)(q-1)} = M(M^{(p-1)(q-1)})^k$
  - If $\gcd(M,p) = 1$, then $M(M^{(p-1)})^{k(q-1)} = M(1)^{k(q-1)} = M \pmod{p}$ by Fermat's Little Theorem
  - If $\gcd(M,p) \neq 1$, then M is a multiple of p, so the message is 0 (mod p)
  - Same for q
  - so, by Chinese Remainder, since $C^e = M \pmod{p}$ and $C^e = M \pmod{q}$, then $C^e = M \pmod{pq}$