Factoring, Math, and RSA

MTH 440

Fermat Factoring

Suppose n is an odd positive integer (if it's not odd divide out by 2's until it is)

1. Let b be the smallest positive integer such that $b^2 \geq n$
2. Let $q = b^2 - n$
3. If q is a perfect square, $q=a^2$, then $n = b^2 - a^2$ and $(b-a)(b+a)$ are factors
4. If q is not a perfect square then replace b^2 with $(b+1)^2$

   If $b + \sqrt{q} > n/2$ stop - n is prime

   Else go back to step 2

We know / saw on the board

- It is easy to compute gcd(a,n)
- It is easy to compute a^{-1} mod n
- It is computationally infeasible to factor n for n large and chosen carefully
  - The current record for factoring an integer of the form n=pq, with p and q prime is n 768 bits (232 digits)

By Fermat's Little Theorem

- For N=pq a product of two distinct primes, define

$$\phi(N) = (p-1)(q-1)$$

- For x relatively prime to N

$$x^{\phi(N)} = 1 \bmod N, \quad \text{so}$$

$$x^{\phi(N)+1} = x \bmod N$$

Hence if $k = 1 \bmod \phi(n)$, then

$$x^k = x \bmod N$$

The RSA Public Key Cipher

- Let $N=pq$ be the product of two very LARGE prime numbers (p and q are kept secret)
  - Typically N is 1024 or 2048 bits
- Choose a secret key d with $0<d<N$
- The public key is (N,e) where $0<e<N$ such that

$$d*e = 1 \bmod \emptyset(N)$$

- Fact: given N and e, it is computationally infeasible to find d without knowledge of either $\emptyset(N)$ or p and q (which are all secret)

BOB

RSA Scheme

ALICE

Alice choose and publishes her public key N,e

To encipher

Bob wishes to send Alice the message M (assume M<N)

$E(M) = M^e \bmod N$

To decipher

Alice computes

$E(M)^d = M^{de} = M \bmod N$

Since de=1 mod $\emptyset$(N), then it should be true that $M^{ed}=M$

N=15, e=11, d=3

Encipher	Decipher
$2^{11} = 2048 = 8\ (15)$	$8^3 = 512 = 2\ (15)$
$3^{11} = 12\ (15)$	$12^3 = 3\ (15)$
$7^{11} = 13\ (15)$	$13^3 = 7\ (15)$
etc.