CIS 3362 10/27/25

RSA Encryption

Rivest Shamir Adleman

Public key(s)

Alice uses Bob's public key to encrypt → Bob

$C = f(M, \text{Bob Public key})$

↑ no one should figure out M given C and Bob's Publickey

Private key(s) ↓ Via these decrypts C to obtain M

Note: Each person who wants to receive messages must set up their own set of Public/Private matching keys.

Adleman walks into Rivest's office but Rivest shows him Diffie-Hellman paper.

Rivest or Shamir would come up with an idea + Adleman would shoot it down.

Party thrown by Grad Student influence lots of Manischewitz Wine, after Rivest got home he had an idea. midnight → whenever WROTE ~~TOOK~~ WHOLE PAPER

Bob will choose 2 large primes p, q.
These are private. Computes $n = pq$, n is Public.
Assuming factoring is hard.
Bob calculates $\phi(n) = (p-1)(q-1)$, this has to be Private

Bob choose a random value, e, such that
$\gcd(e, \phi(n)) = 1$.
↳ e is second Public key

Bob calculates $d \equiv e^{-1} \bmod \phi(n)$, so d is a private key.

Public keys: n, e
Private key: d

Private elements: $p, q, \phi(n)$ (in addition to d)

To encrypt message, M, Alice computes

$$C = M^e \bmod n$$

To read, Bob does $C^d \equiv M \bmod n$ ✓

For now, assume $\gcd(M, n) = 1$. (Note if it didn't, someone could run gcd on C, n and break the system.)

$$(Me)^d = M^{ed} = M^{k\phi(n)+1} = M^{k\phi(n)} \times M^1 = \left(M^{\phi(n)}\right)^k \times M,$$

$ed \equiv 1 \bmod \phi(n)$ for some $k \in \mathbb{Z}$

$\equiv 1^k \times M \equiv M \pmod n$

Given C, e and n, it's difficult to find M s.t. $M^e \equiv C \bmod n$.

Given C, e and n, it's difficult to determine d.

If $\phi(n)$ were known, then you could factor n.

$n = pq$, $\phi(n) = (p-1)(q-1)$

$\phi(n) = n - p - q + 1$

$p + q = \boxed{n + 1 - \phi(n)}$

$q = \boxed{n + 1 - \phi(n) - p}$

$p = 7 \quad q = 13$

$\phi(91) = 6 \times 12 = 72$

$72 = 91 - p - q + 1$

$p + q = 20$

$q = (20 - p)$

C

$n = p(\underline{n + 1 - \phi(n)} - p)$

$n = p(C - p)$

$n = pC - p^2$

$p^2 - pC + n = 0$

$p^2 - Cp + n = 0$

Quadratic in p

$91 = p(20 - p)$

$91 = 20p - p^2$

$p^2 - 20p + 91 = 0$

QUADRATIC

If 2 people use same p, then $n_1 = pq$, $n_2 = pr$, $\gcd(n_1, n_2) = p$ and both systems are broken.

Example

$p = 7 \quad q = 13$

$n = 7 \times 13 = 91$

$\phi(n) = 6 \times 12 = 72$

$e = 5$, $\gcd(72, 5) = 1$

$d = 5^{-1} \bmod 72$

$72 = 14 \times 5 + 2$

$5 = 2 \times 2 + 1$

$5 - 2 \times 2 = 1$

$5 - 2(72 - 14 \times 5) = 1$

$5 - 2 \times 72 + 28 \times 5 = 1$

$29 \times 5 - 2 \times 72 = 1 \bmod 72$

$29 \times 5 \equiv 1 \bmod 72$

$\boxed{d = 29}$

$243 - 182 = 61$

$M = 3 \qquad C = 3^5 \bmod 91$

$= 243 \bmod 91$

$= 61$

Bob $= 61^{29} \bmod 91 \equiv 3 \bmod 91$ ✓

(in IDLE)