10/25/23 - RSA

Diffie-Hellman - Key Exchange (Discrete Log Problem)
↑
Ron Rivest - new faculty member MIT (1975)
read paper.

ONE WAY FUNCTION → easy forwards
hard invert

Convinced Adi Shamir, Leonard ~~Adleman~~ Adleman

GOAL: Public Key Cryptosystem (asymmetric)

Rivest had ideas
Shamir " ideas
Adleman shot them down.
More than a year!
Passover Party 1977 (Mar-Apr)
Overnight → sketched out RSA encryption
Patent → Company → Sold

RSA

Alice wants people to be able to send secure msg to her:

Alice generates 2 private keys : p, q large primes.

Calculate $n = pq$, n will public key (security is based on factoring being hard)

Calculate $\phi(n) = (p-1)(q-1)$ // Private

Alice picks a random e, $\gcd(e, \phi(n)) = 1$

e is another Public key.

Alice computes $d = e^{-1} \bmod \phi(n)$ via EEA.

d is another private key.

$ed \equiv 1 \bmod \phi(n)$

$ed = k\phi(n) + 1$ for some int k

Public : n, e

Private : $p, q, d, (\phi(n))$

rel prime n.

Send to Alice : Pick M $0 < M < n$

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

sends C to Alice.

Alice receives C. Computes $C^d \equiv \boxed{M} \pmod n$

$$C^d = (M^e)^d = M^{ed} = M^{k\phi(n)+1} = (M^{\phi(n)})^k \cdot M \equiv 1 \cdot M \pmod n$$

$n = 11 \times 17 = 187$

$\phi(n) = 10 \times 16 = 160 = 2^4 \times 2 \times 5 = 2^5 \times 5$

$e = 21$ What is d?

$d = 21^{-1} \mod 160$

$$
\begin{aligned}
160 &= 7 \times 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}
$$

$$
\begin{aligned}
&3 - 2 = 1 \\
&3 - (5 - 3) = 1 \\
&2 \times 3 - 1 \times 5 = 1 \\
&2(8 - 5) - 1 \times 5 = 1 \\
&2 \times 8 - 3 \times 5 = 1 \\
&2 \times 8 - 3(13 - 8) = 1 \\
&5 \times 8 - 3 \times 13 = 1 \\
&5(21 - 13) - 3 \times 13 = 1 \\
&\underline{5} \times 21 - \underline{8} \times 13 = 1 \\
&5 \times 21 - 8(160 - 7 \times 21) = 1 \\
&5 \times 21 - 8 \times 160 + 56 \times 21 = 1 \\
&\underline{61} \times 21 - 8 \times 160 = 1 \\
&61 \times 21 \equiv 1 \mod 160
\end{aligned}
$$

$\boxed{d = 61}$

$M = 97$ $\quad C = 97^{21} \equiv 20 \mod 187$ (Alice)

$M = 20^{61} \equiv 97$ Alice computes

Opponent sees $n = 187$, $e = 21$ they have difficulty computing d.

if factor, then $\Rightarrow \phi(n) \Rightarrow d$.

(a) how knowing $\phi(n)$ can help you break it.

(b) Code how to convert text/bits $\rightleftarrows$ M

$$n = 187 = pq$$

$$\phi(n) = 160 = (p-1)(q-1)$$

$$= pq - p - q + 1$$

$$n - \phi(n) = 27 = p + q - 1$$

$$28 = p + q$$

$$q = (28 - p)$$

$$187 = p(28-p)$$

$$187 = 28p - p^2$$

$$p^2 - 28p + 187 = 0$$

Quadratic Formula will work w/ large ints

RSA2.java

$$\text{'CAT'} = 2 \times 26^2 + 0 \times 26^1 \times 19 \times 26^0$$

2 0 19

$$\text{HOME} = 7 \times 26^3 + 14 \times 26^2 + 12 \times 26^1 + 4 \times 26^0$$