CIS 3362 10/30/24

- Diffie-Hellman Key Exchange (1975)

[Ron Rivest read ↑ paper. Really excited.
→ Good can we build on this?

GOAL: BUILD A GEN PUBLIC KEY SCHEME

Alice Public Keys	Alice Private Key
?, ?, ?	?

Bob ⟶ Alice he only uses Alice's Public Keys to create cipher text.
Everyone can read it, but only Alice, with her ~~public~~ private key, can decrypt it.

Ron Rivest
Adi Shamir
} coming up w/ ideas

Leonard Adleman } good at finding the flaws

About 1 year of trying & failing

April 1977

In a single night, Rivest came up with the idea behind RSA.

Sent → Shamir, Adleman

Public Elements

$n = pq$

e, $\gcd(e, \phi(n)) = 1$

$1 < e < n-1$

→ randomly chosen by Alice

Private ~~Keys~~ Elements

p, q → Primes (not keys)

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

$d \equiv e^{-1} \bmod \phi(n)$

→ Private key

How to pick keys

$n = 5 \times 7 = 35$

$\phi(n) = 4 \times 6 = 24$

$e = 11$

$d = 11^{-1} \bmod ~~35~~ 24 = \boxed{11}$

$24 ~~35~~ = ~~3~~ 2 \times 11 + 2$

$11 = 5 \times 2 + 1$

$11 - 5 \times 2 = 1$

$11 - 5(24 - 2 \times 11) = 1$

$11 - 5 \times 24 + 10 \times 11 = 1$

$11 \times 11 - 5 \times 24 = 1$

How to use

Bob Message,

$0 \leq M < n.$

to encrypt

Bob Calculates

$C = M^e \bmod n$

To decrypt, Alice computes

$C^d \bmod n$

$C^d = (M^e)^d \bmod n$

$\equiv M^{ed} \bmod n$

$\equiv M^{k\phi(n)+1} \bmod n$

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

$\rightarrow ed = k\phi(n) + 1$

$\equiv M^{k\phi(n)} \times M \equiv (\bmod n)$

$\equiv (M^{\phi(n)})^k \times M \equiv 1^k M \equiv M \bmod n$

Known Info

n - public key

e - public key

$C = M^e \bmod n$

$C = M^{e} \bmod n$ — e: known; C: known; M: unknown; n: known

Unknown $\phi(n), p, q, d$ } If any of these are uncovered you could break the message

$d \rightarrow$ obvious, just do what Alice would do

$C^d \bmod n$

$p \rightarrow \quad q = \frac{n}{p}, \quad \phi(n) = (p-1)(q-1), \quad d \equiv e^{-1} \bmod \phi(n)$

$q \rightarrow \quad p = \frac{n}{q}, \quad \phi(n) = (p-1)(q-1)$

$\phi(n)$

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

$\phi(n) = (pq - p - q + 1) \qquad q = \frac{n}{p}$

$\phi(n) = n - p - \frac{n}{p} + 1$ — $\phi(n)$: known; n: known

$p\,\phi(n) = pn - p^2 - n + p$ — pn and $+p$: known

$p^2 + (\phi(n) - n - 1)\,p + n = 0$ — $(\phi(n) - n - 1)$: KNOWN; n: KNOWN

Quadratic in only unknown.

Look @ Code

Version 1 - encrypts + decrypts numbers

Version 2 - takes as input block of uppercase characters