

Revisiting the "collision attack" on discrete log.

Working

$$(\mathbb{Z}/p\mathbb{Z})^*$$

List A: $g^{r_1}, g^{r_2}, \dots$ for random r_i 's.

List B: $hg^{-s_1}, hg^{-s_2}, \dots$ random s_i 's

If collision: $g^{r_i} = hg^{-s_j}$

$$\Rightarrow h = g^{r_i + s_j} \text{ discrete log we seek.}$$

Baby-Step-Grant-Step is an "organized" version.

By Birthday Paradox, lists should be expected to be $O(\sqrt{p})$ in length for a collision.

Birthday Paradox

r people / random list of elements

N days of year / possible values

Q: any repeats?

Prob of ^{no} repeats:

$$\left(1 - \frac{1}{N}\right) \left(1 - \frac{2}{N}\right) \left(1 - \frac{3}{N}\right) \cdots \left(1 - \frac{r-1}{N}\right)$$

prob that
2nd doesn't
match 1st

prob 3rd
doesn't
repeat
1st or 2nd

r^{th} person

$$\approx 1 - e^{-\frac{r^2}{2N}}$$

drops below $\frac{1}{2}$ around $\frac{r^2}{2N} \sim .8$ i.e. $r \sim O(\sqrt{N})$

The RSA Algorithm

Rivest, Shamir, Adelman

(British secretly: Ellis, Cocks)

Alice

Encryption

Bob

message $0 < m < n$

encryption:

$$c \equiv m^e \pmod{n}$$

Setup: primes p, q (secret!)

$$\text{let } n = p \cdot q$$

choose $e \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$

and compute $d \equiv e^{-1} \pmod{\varphi(n)}$

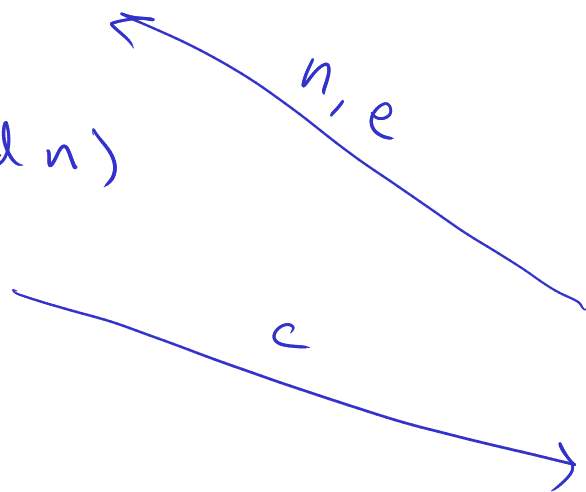
Private: d (decryption exponent)

Public key: $\begin{cases} n \text{ (modulus)} \\ e \text{ (encryption exponent)} \end{cases}$

decryption:

$$m \equiv c^d \pmod{n}$$

$$\equiv (m^e)^d \equiv m^{ed} \equiv m'$$



Security of RSA

Eve sees: $n, e, c \equiv m^e \pmod{n}$

① If Eve can get $\phi(n)$, she can compute $d \equiv e^{-1} \pmod{\phi(n)}$
 $\Rightarrow$ obtains secret key

② If Eve can get p, q , she can $\phi(n) = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) = (p-1)(q-1)$
 $\Rightarrow$ use ①

So: Factoring n breaks RSA.

Q: Is getting $\phi(n)$ easier than factoring n (a product of 2 primes)?

If Eve has $\phi(n)$, she can factor n .

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

$$\begin{aligned} \text{So } p, q \text{ are roots of } (X-p)(X-q) &= X^2 - (p+q)X + pq \\ &= X^2 - (n - \phi(n) + 1)X + n \end{aligned}$$

* use quadratic formula to get p, q .

(factoring a product n of 2 primes) is equivalent to (computing $\mathcal{C}(n)$)
in polynomial time.

More observations:

- If Eve can compute d , she can compute $\mathcal{C}(n)$
 - we'll see a probabilistic alg. for this
 - 2004, Coron, May: $\exists$ a deterministic algorithm
- Not known if finding m is equivalent to factoring.

Attacks:

- attacks on factoring
- on special choices of parameters (e.g. small message or small e)
- on implementation

Example. Solve $x^2 \equiv 1 \pmod{35}$

$$\overset{\text{CRT}}{\iff} \text{Solve } \begin{cases} x^2 \equiv 1 \pmod{5} \\ x^2 \equiv 1 \pmod{7} \end{cases}$$

$$\iff \begin{cases} x \equiv \pm 1 \pmod{5} \\ x \equiv \pm 1 \pmod{7} \end{cases}$$

$$\iff \begin{pmatrix} x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} \end{pmatrix} \text{ or } \begin{pmatrix} x \equiv -1 \pmod{5} \\ x \equiv 1 \pmod{7} \end{pmatrix} \text{ or } \begin{pmatrix} x \equiv 1 \pmod{5} \\ x \equiv -1 \pmod{7} \end{pmatrix} \text{ or } \begin{pmatrix} x \equiv -1 \pmod{5} \\ x \equiv -1 \pmod{7} \end{pmatrix}$$

$$\overset{\text{CRT}}{\iff} x \equiv 1, 29, 6, 34 \equiv -1$$