Algorithms related to Factoring and Discrete-log

Definition (Collection of one-way functions)

- a collection of one-way functions is a family $F = \{f_j : D_j \to R_j\}_{j \in J}$ if:
    1. It is easy to sample $j \in J$ to get a f_j
    2. It is easy to sample uniformly from D_j
    3. Easy to evaluate
    4. Hard to invert

$$\Pr[j \leftarrow Gen(1^n), x \leftarrow D_j, y = f_j(x), x' = A(1^n, j, y) : f_j(x') = y] \leq \epsilon(n) \tag{1}$$

RSA Problem

- Let $\Pi_n = \{q | 2 < q < 2^n, q \text{ prime}\}$, $p, q \leftarrow \Pi_n, N = pq$.
- Let $e \leftarrow \mathbb{Z}^*_{\Phi(N)}$ ($\Phi(N) = (p-1)(q-1)$), and where $\mathbb{Z}^*$ is the multiplicative group.
- Let $y \leftarrow \mathbb{Z}^*_N$.
- RSA problem: Given N, e, y, find x from $\mathbb{Z}^*_N$ such that

$$x^e = y \bmod N \tag{2}$$

- RSA assumption: $f_{N,e}(x) = x^e \bmod N$ is a collection of one-way function.
- If we know the inverse element d of e: $de = 1 \bmod \Phi(N)$, then $x = y^d \bmod N$. And d can be derived from $\Phi(N)$
- **Observation**: Breaking factoring problem helps finding $\Phi(N)$ and thus d, which breaks RSA problem.

Public-key encryption scheme

- Public key N, e
- Private key N, d
- Encrypt: $Enc(pk, m) = m^e \bmod N$

Generalization of RSA

- Let N be a composite integer of unknown factorization, let

$$p(x) = x^\delta + a_{\delta-1}x^{\delta-1} + \cdots + a_0 \tag{3}$$

  be a monic integer polynomial of degree δ.
- Given $p()$, N, find a root of $p(x)$ mod N.

Another variant of RSA

- Instead of finding x, find e in:

$$x^e = y \bmod N \tag{4}$$

The Rabin Problem

- Change $e \in \mathbb{Z}^*_{\Phi(N)}$ in RSA problem to $e = 2$.
- Let $y \leftarrow QR_N$
- Given N, y, find x from $\mathbb{Z}^*_N$ such that

$$x^2 = y \bmod N \tag{5}$$

- **Theorem:** Breaking Rabin problem = Breaking Factoring

Discrete-log Problem

- Let q be a **prime modulus** such that $q - 1$ has a large prime factor p, then let G be a subgroup of $\mathbb{Z}^*_q$ of order p
- For example, let $q = 2p + 1$ where p, q are primes
- For a random $x \in \mathbb{Z}_p$, Let (g is a generator of G)

$$y = g^x \bmod q \tag{6}$$

-
- The discrete-log problem: Given G, g, y find x.

Diffie-Hellman key agreement from discrete-log

- See One note