Public key encryption from Diffie-Hellman

A Unifying Theme

One-way functions (informal)

A function $f: X \longrightarrow Y$ is one-way if

- There is an efficient algorithm to evaluate $f(\cdot)$, but
- Inverting f is hard:

for all efficient A and $x \longleftarrow X$:

$$\Pr\Big[\quad A\big(f(x)\big) \qquad\qquad \Big] < \text{negligible}$$

Functions that are not one-way: $f(x) = x$, $f(x) = 0$

Ex. 1: generic one-way functions

Let $f: X \longrightarrow Y$ be a secure PRG (where $|Y| \gg |X|$)

(e.g. f built using det. counter mode)

Lemma: f a secure PRG $\Rightarrow$ f is one-way

Proof sketch:

A inverts f $\Rightarrow$ B(y) = is a distinguisher

Generic: no special properties. Difficult to use for key exchange.

Ex 2: The DLOG one-way function

Fix a finite cyclic group G (e.g $G = (Z_p)^*$) of order n

g: a random generator in G (i.e. $G = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$)

Define: $f: Z_n \longrightarrow G$ as $\boxed{f(x) = g^x \in G}$

Lemma: Dlog hard in G $\Rightarrow$ f is one-way

Properties: $f(x), f(y) \Rightarrow f(x+y) =$

$\Rightarrow$ key-exchange and public-key encryption

Ex. 3: The RSA one-way function

- choose random primes p,q ≈1024 bits. Set **N=pq**.
- choose integers **e , d** s.t. **e⋅d = 1 (mod φ(N))**

Define: f: $\mathbb{Z}_N^* \to \mathbb{Z}_N^*$ as $\boxed{f(x) = x^e \quad \text{in } \mathbb{Z}_N}$

Lemma: f is one-way under the RSA assumption

Properties: f(x⋅y) = f(x) ⋅ f(y) and **f has a trapdoor**

Summary

Public key encryption:

made possible by one-way functions
with special properties

homomorphic properties and trapdoors

End of Segment