2. Problems in public key

Problems

Easy problems

> Generating random elements

Given

- N
- $x \in \mathbb{Z}_N$

> find $x^{-1} \in \mathbb{Z}_N$ - Extended euclidean algorithm

Given

- prime p
- $f(x) \in \mathbb{Z}_p[x]$

> find $x \in Z_p \ s.t \ f(x) \bmod 0 \bmod p$ - $\mathcal{O}(deg(f))$

Hard problems

We consider a hard problem hard if the probability of all **efficient** adversaries to solve the problem is neglijable

In $\mathbb{Z}_p$:

Discrete log problem
Let

- g be a generator of $\mathbb{Z}_p^*$

> Given $x \in \mathbb{Z}_p^*$ find a number $r \ s.t. \ x \equiv g^r \bmod p \iff r \equiv DLog_g(g^r) \bmod p$

ECDLP
Let

- G be a generator point of $E(\mathbb{Z}_p)$

> given $P \in E(\mathbb{Z}_p)$ find a number $r \ s.t. \ P = r \cdot G \iff r \equiv DLog_G(r \cdot G)$

- Harder than DLP

Diffie-Hellman problem
Let

- g be a generator of $\mathbb{Z}_p^*$

> Given $x, y \in \mathbb{Z}_p^*$ where
>
> - $x = g^{r_1}$ and $y = g^{r_2}$.
>
> Find $z = g^{r_1 r_2}$

In $\mathbb{Z}_n$:

Problems based on the hardness of factorization

> Given n factorize it into primes

> Test if an element is QR in $\mathbb{Z}_n$

> Square root in $\mathbb{Z}_n$ (like factoring n).

> e'th roots modulo n when $\gcd(e, \varphi(n)) = 1$

> Solving polynomial equations of degree $d > 1$.
>
> - If factorization is known find roots mod primes and CRT to win

DLP in $\mathbb{Z}_n$

Diffie hellman problem in $\mathbb{Z}_n$