2. Problems in public key

Problems

Easy problems

Examples of easy problems

1. Generating random elements
2. Inverse of a number modulo. Given
   - N
   - $x \in \mathbb{Z}/N\mathbb{Z}$

   find $x^{-1} \in \mathbb{Z}/N\mathbb{Z}$ - Extended euclidean algorithm
3. Roots of polynomials in polynomial rings modulo prime numbers
   Given
   - prime p
   - $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$

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

Hard problems

We consider a problem hard if for all **efficient** adversaries the probability to solve the problem is negligible.

In $\mathbb{Z}/p\mathbb{Z}$ where p is prime:

1. **Discrete log problem**
   Given
   - g be a generator of $\mathbb{Z}/p\mathbb{Z}^*$
   - $h \in \mathbb{Z}/p\mathbb{Z}^*$

   find a number $x \text{ such that. } h \equiv g^x \bmod p$.
2. **ECDLP**
   Given
   - G be a generator point of an elliptic curve over a prime field $E(\mathbb{Z}/p\mathbb{Z})$
   - a point $P \in E(\mathbb{Z}_p)$

   find a number $x \text{ such that. } P = x \cdot G$. This is considered harder than DLP
3. **Diffie-Hellman problem**
   Given
   - g be a generator of $\mathbb{Z}_p^*$
   - $h_1, h_2 \in \mathbb{Z}/p\mathbb{Z}^*$ where
   - $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$.

   find $z = g^{x_1 x_2}$.

In $\mathbb{Z}/n\mathbb{Z}$:

Problems based on the hardness of factorization

1. Given n factorize it into primes
2. Test if an element is a quadratic residue in $\mathbb{Z}/n\mathbb{Z}$
3. Square root in $\mathbb{Z}/n\mathbb{Z}$ (as hard as factoring n).
4. e'th roots modulo n when $\gcd(e, \varphi(n)) = 1$
5. Solving polynomial equations of degree $d > 1$.
   - If factorization is known find roots mod primes and CRT to win.

DLP in $\mathbb{Z}/n\mathbb{Z}$

Diffie hellman problem in $\mathbb{Z}/n\mathbb{Z}$