

Computationally hard problems in number theory

Paul Dumais, October 2002

See *Handbook of Applied Cryptography* table 3.1.

1 FACTORING

Input: $n \geq 1$

Output: the prime factorization of n

2 RSA

Input: an integer n that is the product of two distinct odd primes, $e \in \mathbb{Z}_{\phi(n)}^*$, $y \in \mathbb{Z}_n$

Output: $x \in \mathbb{Z}_n$ such that $x^e \bmod n = y$

3 QR (*quadratic residuosity*)

Input: an odd composite integer n , $a \in \mathbb{Z}_n$ such that $\left(\frac{a}{n}\right) = 1$

Output: “ $a \in Q_n$ ” or “ $a \in \bar{Q}_n$ ”

4 SQROOT (*square root*)

Input: a composite integer n , $x \in Q_n$

Output: $z \in \mathbb{Z}_n^*$ such that $z^2 \bmod n = x$

5 DL (*discrete logarithm*)

Input: $p \in \mathbb{P}$, g a generator of \mathbb{Z}_p^* , $\alpha \in \mathbb{Z}_p^*$

Output: a such that $0 \leq a \leq p - 2$ and $g^a \bmod p = \alpha$

6 DH (*Diffie-Hellman*)

Input: $p \in \mathbb{P}$, g a generator of \mathbb{Z}_p^* , $\alpha \in \mathbb{Z}_p^*$, $\beta \in \mathbb{Z}_p^*$

Output: $g^{ab} \bmod p$ where $g^a \bmod p = \alpha$ and $g^b \bmod p = \beta$