Easy DL

THEOREM 5.9 (Euler's Criterion) *Let p be an odd prime. Then a is a quadratic residue modulo p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

PROOF First, suppose $a \equiv y^2 \pmod{p}$. Recall from Corollary 5.6 that if p is prime, then $a^{p-1} \equiv 1 \pmod{p}$ for any $a \not\equiv 0 \pmod{p}$. Thus we have

$$\begin{aligned} a^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \pmod{p} \\ &\equiv y^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Conversely, suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Let b be a primitive element modulo p. Then $a \equiv b^i \pmod{p}$ for some positive integer i. Then we have

$$\begin{aligned} a^{(p-1)/2} &\equiv (b^i)^{(p-1)/2} \pmod{p} \\ &\equiv b^{i(p-1)/2} \pmod{p}. \end{aligned}$$

Since b has order $p-1$, it must be the case that $p-1$ divides $i(p-1)/2$. Hence, i is even, and then the square roots of a are $\pm b^{i/2} \bmod p$. ∎

The Diffie-Hellman Problems

Problem 6.3:	Computational Diffie-Hellman
Instance:	A multiplicative group $(G, \cdot)$, an element $\alpha \in G$ having order n, and two elements $\beta, \gamma \in \langle \alpha \rangle$.
Question:	Find $\delta \in \langle \alpha \rangle$ such that $\log_\alpha \delta \equiv \log_\alpha \beta \times \log_\alpha \gamma \pmod{n}$. (Equivalently, given α^b and α^c, find α^{bc}.)

CDH

Problem 6.4:	Decision Diffie-Hellman
Instance:	A multiplicative group $(G, \cdot)$, an element $\alpha \in G$ having order n, and three elements $\beta, \gamma, \delta \in \langle \alpha \rangle$.
Question:	Is it the case that $\log_\alpha \delta \equiv \log_\alpha \beta \times \log_\alpha \gamma \pmod{n}$? (Equivalently, given α^b, α^c and α^d, determine if $d \equiv bc \pmod{n}$.)

DDH

Computational Diffie-Hellman $\propto_T$ Discrete Logarithm.

CDH $\leq$ DL

find $b = \log_\alpha \beta$ and $c = \log_\alpha \gamma$.

compute $d = bc \bmod n$ and $\delta = \alpha^d$.

given $\alpha^b, \alpha^c, \alpha^d$
test if $d \equiv bc \bmod n$

Given α^b, α^c find α^{bc}

Decision Diffie-Hellman $\propto_T$ Computational Diffie-Hellman

find the value δ' such that

$$\log_\alpha \delta' \equiv \log_\alpha \beta \times \log_\alpha \gamma \pmod{n}.$$

Then check to see if $\delta' = \delta$.

DDH $\leq$ CDH

ElGamal $K = \{(p, \alpha, a, \beta) : \beta = \alpha^a \bmod p\}$

Encr. $y_1 = \alpha^k$

$y_2 = x\beta^k$

Decr. $x = y_2 (y_1^a)^{-1} \bmod p$

$\delta = \text{ORACLECDH}(\alpha, \beta, y_1), \quad = \alpha^{ka} = y_1^a$

$x = y_2 \delta^{-1}.$

ElGamal $\leq$ CDH

$x = \text{ORACLEELGAMALDECRYPT}(\alpha, \beta, (y_1, y_2))$,

$\delta = y_2 x^{-1}$)

CDH ≤ ElGamal

DDH ≤ CDH ≤ DL

=

ElGamal