The discrete logarithm problem in $\mathbb{Z}_p$

Problem Instance $I = (p, \alpha, \beta)$, where p is prime, $\alpha \in \mathbb{Z}_p$ is a primitive element, and $\beta \in \mathbb{Z}_p^*$.

Objective Find the unique integer a, $0 \leq a \leq p-2$, such that

$$\alpha^a \equiv \beta \pmod{p}.$$

We will denote this integer a by $\log_\alpha \beta$.

Cryptosystem 6.1: *ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$*

Let p be a prime such that the Discrete Logarithm problem in $(\mathbb{Z}_p^*, \cdot)$ is infeasible, and let $\alpha \in \mathbb{Z}_p^*$ be a primitive element. Let $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, and define

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}.$$

The values p, α and β are the public key, and a is the private key.

For $K = (p, \alpha, a, \beta)$, and for a (secret) random number $k \in \mathbb{Z}_{p-1}$, define

$$e_K(x, k) = (y_1, y_2),$$

where

$$y_1 = \alpha^k \bmod p$$

and

$$y_2 = x\beta^k \bmod p.$$

For $y_1, y_2 \in \mathbb{Z}_p^*$, define

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

$\mathbb{Z}_n$ represents three alphabetic characters as in the following examples:

$$
\begin{array}{lcll}
DOG & \rightarrow & 3 \times 26^2 + 14 \times 26 + 6 & = 2398 \\
CAT & \rightarrow & 2 \times 26^2 + 0 \times 26 + 19 & = 1371 \\
ZZZ & \rightarrow & 25 \times 26^2 + 25 \times 26 + 25 & = 17575.
\end{array}
$$

$26^3 = 17576$

Z_p

FIGURE 5.3
Shanks' algorithm for the discrete logarithm problem

1. Compute $\alpha^{mj} \bmod p, 0 \leq j \leq m-1$
2. Sort the m ordered pairs $(j, \alpha^{mj} \bmod p)$ with respect to their second coordinates, obtaining a list L_1
3. Compute $\beta\alpha^{-i} \bmod p, 0 \leq i \leq m-1$
4. Sort the m ordered pairs $(i, \beta\alpha^{-i} \bmod p)$ with respect to their second coordinates, obtaining a list L_2
5. Find a pair $(j, y) \in L_1$ and a pair $(i, y) \in L_2$ (i.e., a pair having identical second coordinates)
6. define $\log_\alpha \beta = mj + i \bmod (p-1)$.

Example 6.2 Suppose we wish to find $\log_3 525$ in $(\mathbb{Z}_{809}{}^*, \cdot)$. Note that 809 is prime and 3 is a primitive element in $\mathbb{Z}_{809}{}^*$, so we have $\alpha = 3$, $n = 808$, $\beta = 525$ and $m = \lceil \sqrt{808} \rceil = 29$. Then

$$\alpha^{29} \bmod 809 = 99.$$

First, we compute the ordered pairs $(j, 99^j \bmod 809)$ for $0 \leq j \leq 28$. We obtain the list

$(0, 1)$	$(1, 99)$	$(2, 93)$	$(3, 308)$	$(4, 559)$
$(5, 329)$	$(6, 211)$	$(7, 664)$	$(8, 207)$	$(9, 268)$
$(10, 644)$	$(11, 654)$	$(12, 26)$	$(13, 147)$	$(14, 800)$
$(15, 727)$	$(16, 781)$	$(17, 464)$	$(18, 632)$	$(19, 275)$
$(20, 528)$	$(21, 496)$	$(22, 564)$	$(23, 15)$	$(24, 676)$
$(25, 586)$	$(26, 575)$	$(27, 295)$	$(28, 81)$	

which is then sorted to produce L_1.

The second list contains the ordered pairs $(i, 525 \times (3^i)^{-1} \bmod 809)$, $0 \leq j \leq 28$. It is as follows:

$(0, 525)$	$(1, 175)$	$(2, 328)$	$(3, 379)$	$(4, 396)$
$(5, 132)$	$(6, 44)$	$(7, 554)$	$(8, 724)$	$(9, 511)$
$(10, 440)$	$(11, 686)$	$(12, 768)$	$(13, 256)$	$(14, 355)$
$(15, 388)$	$(16, 399)$	$(17, 133)$	$(18, 314)$	$(19, 644)$
$(20, 754)$	$(21, 521)$	$(22, 713)$	$(23, 777)$	$(24, 259)$
$(25, 356)$	$(26, 658)$	$(27, 489)$	$(28, 163)$	

After sorting this list, we get L_2.

Now, if we proceed simultaneously through the two sorted lists, we find that $(10, 644)$ is in L_1 and $(19, 644)$ is in L_2. Hence, we can compute

$$\begin{aligned} \log_3 525 &= (29 \times 10 + 19) \bmod 808 \\ &= 309. \end{aligned}$$

Problem 6.1:	Discrete Logarithm
Instance:	A multiplicative group $(G, \cdot)$, an element $\alpha \in G$ having order n, and an element $\beta \in \langle \alpha \rangle$.
Question:	Find the unique integer a, $0 \leq a \leq n-1$, such that $$\alpha^a = \beta.$$ We will denote this integer a by $\log_\alpha \beta$.

FIGURE 5.9
Generalized ElGamal Public-key Cryptosystem

Let G be a finite group with group operation $\circ$, and let $\alpha \in G$ be an element such that the discrete log problem in H is intractible, where $H = \{\alpha^i : i \geq 0\}$ is the subgroup generated by α. Let $\mathcal{P} = G$, $\mathcal{C} = G \times G$, and define

$$\mathcal{K} = \{(G, \alpha, a, \beta) : \beta = \alpha^a\}.$$

The values α and β are public, and a is secret.

For $K = (G, \alpha, a, \beta)$, and for a (secret) random number $k \in \mathbb{Z}_{|H|}$, define

$$e_K(x, k) = (y_1, y_2),$$

where

$$y_1 = \alpha^k$$

and

$$y_2 = x \circ \beta^k.$$

For a ciphertext $y = (y_1, y_2)$, define

$$d_K(y) = y_2 \circ (y_1^a)^{-1}.$$

Easy log

(1) $(Z_7, +)$ $\alpha = 1$

$$\alpha^k = k \bmod 7$$

$$\log_\alpha k = k$$

(2) $Z_2[x]/x^3+x+1$ $GF(8)^*$

$\{1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

Cyclic with $\alpha = x$

$x, \; x^2 = x^2, \; x^3 = x+1, \; x^4 = x^2+x, \ldots$

$x^5 = x^2+x+1, \quad x^6 = x^2+1, \quad x^7 = 1$

Algorithm 6.1: SHANKS(G, n, α, β)

1. $m \leftarrow \lceil \sqrt{n} \rceil$
2. **for** $j \leftarrow 0$ **to** $m - 1$
   do compute α^{mj}
3. Sort the m ordered pairs (j, α^{mj}) with respect to their second coordinates, obtaining a list L_1
4. **for** $i \leftarrow 0$ **to** $m - 1$
   do compute $\beta\alpha^{-i}$
5. Sort the m ordered pairs $(i, \beta\alpha^{-i})$ with respect to their second coordinates, obtaining a list L_2
6. Find a pair $(j, y) \in L_1$ and a pair $(i, y) \in L_2$ (i.e., find two pairs having identical second coordinates)
7. $\log_\alpha \beta \leftarrow (mj + i) \bmod n$