Alg. for solving the DLP:

c) Pohlig-Hellman-Method:

Assumption: Factorization of n is known: $n = \prod_{i=1}^{r} p_i^{e_i}$

Idea: Solve DLPs in subgroups of order $p_i^{e_i}$, hence, compute $a_i \bmod p_i^{e_i}$, then use CRT to compute $a \bmod n$

The DLP in the subgroup of order $p_i^{e_i}$ can be reduced to e_i DLPs in the subgroup of order p_i.
Solve these DLP with b).
(For more details MOV)

Complexity $\sum_{i=1}^{r} e_i \big(\underbrace{\log(n)}_{\text{reduction}} + \underbrace{\sqrt{p_i}}_{\text{BSGS}}\big) + \underbrace{(\log(n))^2}_{\text{CRT}}$ operations

→ complexity depends on the largest prime divisor of n
→ for cryptographic purposes choose groups with a large prime divisor
→ If n is prime it is just b) (BSGS)

d) Pollard: ρ-method

Idea: Find numbers $c, d, c', d' \in \mathbb{Z}$ s.t.

$$cP + d\cdot Q = c'P + d'\cdot Q$$
$$\Rightarrow (c - c')\cdot P = (d' - d)\,Q = (d' - d)\,aP$$
$$\Rightarrow (c - c') \equiv (d' - d)\cdot a \pmod n$$

If $\gcd(d' - d, n) = 1$, compute $(d' - d)^{-1}(c - c') = a \pmod n$
$\Rightarrow Q = aP$

To find such numbers, construct pseudo-random sequences c_i, d_i
$x_i = c_i P + d_i Q$. On a finite set a collision will occur.

Therefore, the method is called ρ-method.
(As the values of x_i look like a ρ.)

Complexity: $O(\sqrt{n})$

– Specialized method using some more structure

e) Reduction algorithm for ECDLP (MOV / Frey–Rück):
Reduce ECDLP in $E(\mathbb{F}_q)$ to a DLP in $\mathbb{F}_{q^k}^*$ for some $k \in \mathbb{N}$ (embedding degree).
↳ Can be avoided by choice of E leading to large k.

f) Index Calculus (similar to sieving methods for factorizing integers)

Idea: Use a factorbase $\alpha^a = \prod_{i=1}^{t} p_i^{\lambda_i}$, where α is generator, a is random number and $(p_1, \dots, p_t)$ is factor base of t primes.

It follows that $a = \sum_{i=1}^{t} \lambda_i \log_\alpha(p_i)$

Choose factorbase with small elements, s.t., sufficiently many group elements can be represented as a product of element of this factorbase

Compute DLs for these elements.

Obtain a system of linear equations by taking enough random numbers a and getting enough equations & solve it to obtain the solution of the DLP

- Most efficient alg. known for $\mathbb{F}_p$ (and $\mathbb{F}_{q^k}^*$)
  subexponential complexity $e^{\sqrt[3]{\frac{64}{9}} (\log(n))^{1/3} (\log(\log(n)))^{2/3}}$
  comparison to $\sqrt{n} = n^{1/2} = e^{\ln(n^{1/2})} = e^{1/2 \ln(2) \log(n)}$
- Index calculus cannot be applied to $E(\mathbb{F}_q)$, problem is the construction of the factor base

<u>Cryptographically secure curves</u>

Choose a cyclic group $\langle P \rangle \subseteq E(\mathbb{F}_q)$, s.t.
- $\langle P \rangle$ contains at least 2^{160} points ((a), (b), (d) not feasible)
- $\mathrm{ord}(P) = |\langle P \rangle|$ has a prime factor of size 2^{160} ((c) not feasible)
- embedding degree k should be large ((e) is not feasible)

Comparison DLP vs. ECDLP

There exist more efficient alg. for solving the DLP in $\mathbb{F}_p^*$ and $\mathbb{F}_q^*$ than for $E(\mathbb{F}_q)$, hence, ECC has a security advantage. The following systems have the same security level (keylength. comp.):

DL on $\mathbb{F}_p^*$	ECDL
p : 2048 Bits	n : 224 Bits
q : 224 Bits (group order	

13.4 Cryptographic Applications

Having selected a cryptographically secure curve, carry out protocols based on the ECDLP:

Prerequisites: $\langle P \rangle \leq E(\mathbb{F}_q)$, $\mathrm{ord}(P) = n$, publically known

13.4.1 DH key exchange

13.4.2. Mapping of Integers to points of elliptic curves and vice versa

The mapping of integers to elements of the group $\langle P \rangle$ will be described in two steps. First, a deterministic approach for a special case. Second, a probabilistic approach for the general case

Deterministic procedure

Let $\quad E: y^2 = x^3 + ax \cancel{+b} \quad a, b \in \mathbb{F}_p$

be an elliptic curve over $\mathbb{F}_p$ with $\underline{b = 0}$ and prime $p \equiv 3$ (mod 4

For a message $0 < M < p/2$, let $x = M$

- Calculate $z = x^3 + a \cdot x$
- If z is quadratic residue, calculate a square root $y \bmod p$, which can be easily done, cf. Prop. 9.3.
- Otherwise, repeat the last two calculations for $x = p - M$

The point on the elliptic curve is (x, y)

This procedure is valid:

If M or $p - M$ is a quadratic residue, the validity is obvious. It remains to show that either M or $p - M$ is quadratic residue. Let g be a generator, then there exists $0 < i < p$, s.t.

$$M^3 + aM \equiv g^i \pmod p$$

If i is even, $z = M^3 + aM \bmod p$ is a quadratic residue. Otherwise, if i is odd then

$$(p-M)^3 + a(p-M) \equiv -M^3 - aM \equiv -g^i \overset{(*)}{\equiv} g^{i+\frac{p-1}{2}} \pmod p$$

As $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd, i.e., $i + \frac{p-1}{2}$ is even.

Hence, $z = (p-M)^3 + a(p-M) \bmod p$ is a quadratic residue

<u>Remark on (*)</u>:

As $\mathbb{F}_p$ is a field, the square roots of $1 \equiv g^0 \equiv g^{p-1} \pmod p$ is either 1 or $-1 \equiv g^{\frac{p-1}{2}} \pmod p$. Hence, $-g^i \equiv g^{i+\frac{p-1}{2}} \pmod p$

Let (x, y) a point on the ECC, then the corresponding message is given as $M = \min(x, p-x)$.

Probabilistic procedure

Let E be an arbitrary EC, $k \in \mathbb{N}$, determining the prob. of failure (or the width of the interval of messages.)
$SQR(z, p)$ returns a square root of $z \bmod p$.

Alg. 13 | Mapping of a Message M on a point of an EC E

Input: $E/\mathbb{F}_p$, $0 < M < \frac{p}{2^k}$

Output: A point (x, y) on the EC E with prob. $1 - \frac{1}{2^{2^k}}$

```
i ← 0
repeat
    x ← 2^k · M + i
    z ← x^3 + ax + b mod p
    i ← i + 1
until i ≥ 2^k or z is quadratic residue
if z is quadratic residue then
    y ← SQR(z, p)
    return (x, y)
else
    return FAIL
endif
```