# ZKDL Camp Topics

## Basic Topics (Preliminaries)

1. **Mathematics for cryptographers.**
   (a) Basics of number theory, RSA case study.
   (b) Definition of a group. Subgroups, cyclic groups, isomorphisms and automorphisms. Applications.
   (c) Vector spaces.
   (d) Polynomials.
   (e) Definition of a field. Finite fields.
2. **Elliptic Curves.**
   (a) Defining a group structure.
   (b) Points addition in affine form.
   (c) Scalar multiplication, effective implementation in $O(\log_2(k))$.
   (d) Twisted Curves.
   (e) Useful endomorphism.
   (f) Examples of widely used curves.
3. **Elliptic Curve Pairings** (*might simply redirect to the zksync lecture*).
   (a) Definition and applications.
   (b) Finite field extensions $\mathbb{F}_{p^n}$.
   (c) *(optional, possibly advanced topic)* Implementation details: divisors, ate pairing, Miller Loop.
4. **Cryptographic Commitments**.
   (a) Hash and Pedersen commitments.
   (b) Functional commitments: Polynomial commitments.
   (c) KZG commitment scheme.
   (d) $\tau$ ceremony.

## Medium Topics

1. Introduction: What are zero-knowledge proofs? Basic examples.
2. Succinct Non-Interactive Arguments of Knowledge (SNARK): what succinctness means and security definitions.
3. Arithmetic Circuits. Rank-1 Constraint Systems. Quadratic Arithmetic Programs.
4. Programming SNARKs. Circom. Solving real-world problems with Circom and many practical examples.
5. Zero-knowledge proving systems case studies:
   (a) Groth16
   (b) Plonk
   (c) Range proofs + Bulletproofs + Bulletproofs+ + Bulletproofs++
   (d) STARKs

## Advanced topics

1. Low-level arithmetic and optimizations.
2. Halo2.
3. Nova, Supernova, Hypernova.
4. Folding schemes.