1. (a) (2p) Describe which problem a digital signature scheme is supposed to solve.
   (b) (2p) Explain why a hash function is typically used in a digital signature scheme.
   (c) (4p) Describe the RSA digital signature scheme.
   (d) (2p) Describe a man-in-the-middle attack, and say something about the protection a digital signature scheme gives against such attacks.

2. (a) (3p) How many steps are needed to complete a Miller-Rabin test? Does the algorithm run in polynomial/subexponential/exponential time.

   (b) (1p) Does the quadratic sieve algorithm run in polynomial, subexponential, or exponential time?

   (c) (2p) What is the running time of the best algorithm (currently known) that solves the Elliptic Curve DLPs over $\mathbb{F}_p$? Classify whether the algorithm runs in polynomial, subexponential or exponential time.

   (d) (3p) What is the fastest way to solve a DLP $g^x \equiv_p h$ with p a prime of the form $p = 1 + 2^k$. Does that algorithm run in polynomial, subexponential, or exponential time?

   (e) (1p) Suppose an algorithm takes an input with k bits and requires $\mathcal{O}\left(e^{\sqrt{\log k}}\right)$ steps to complete. Classify whether the algorithm runs in polynomial/subexponential/exponential time.

3. (a) (1p) What kind of problem does the index calculus method solve?
   (b) (1p) What is a B-smooth number?
   (c) (5p) Give an overview of the index calculus method.
   (d) (1p) Does the index calculus method run in polynomial, subexponential or exponential time?
   (e) (2p) Explain why the complexity of the index calculus method depends on the distribution of B-smooth numbers.

4. Let E be an elliptic curve over $\mathbb{F}_p$.

   (a) (2p) What does the Hasse bound (Hasse's theorem) tell us about how many points $E(\mathbb{F}_p)$ can have.

   (b) (1p) Does the fastest known algorithm to compute the number of points of $E(\mathbb{F}_p)$ run in polynomial, subexponential, or exponential time?

   (c) (1p) One application of elliptic curves in cryptography is the elliptic ElGamal cryptosystem. Explain why it can be important to be able to compute the number of points of $E(\mathbb{F}_p)$ to set up the elliptic ElGamal cryptosystem.

   (d) (1p) One application of elliptic curves in cryptography is the elliptic ElGamal cryptosystem. Explain why it is not obvious how to encode messages when using elliptic ElGamal cryptosystem.

   (e) (5p) Another application is Lenstra's factorization algorithm. Explain why Lenstra's factorization algorithm (in general) is faster than Pollard's $p - 1$ factorization algorithm even though they are based on the same idea.