1. (a) (3p) Describe the Elliptic curve Diffie Hellman key exchange (ECDH).

   (b) (2p) Give a short description how to set up the ECDH, i.e. how to choose the public parameters.

   (c) (2p) What is the algorithm involved in computing the shared secret key in ECDH? What is its complexity? Is it polynomial/subexponential/exponential?

   (d) (3p) Explain what the main reason are for ECDH being preferred over the usual DH (in $\mathbb{F}_p^*$).

2. (a) (1p) What is probabilistic encryption?
   (b) (3p) What are the security problems connected with using a deterministic cryptosystem?
   (c) (2p) What is it that makes the encryption of the ElGamal cryptosystem probabilistic?
   (d) (1p) Name a drawback with probabilistic encryption compared to determinstic encryption?
   (e) (3p) Describe how to use padding to make the encryption of the RSA cryptosystem into a probabilistic one.

3. (a) (2p) How many steps are needed to do a Fermat primality test? Does the algorithm run in polynomial/subexponential/exponential time.

   (b) (1p) Does the quadratic sieve algorithm to factorise a composite number N run in polynomial, subexponential, or exponential time?

   (c) (2p) For which choices of N is Pollard's $p-1$ factorization algorithm fast?

   (d) (3p) What is the complexity of Shank's Babystep-Giantstep algorithm and what is the complexity of the naive method to solve a DLP? Classify whether these algorithms run in polynomial, subexponential or exponential time.

   (e) (2p) What is the complexity of the Pollard ρ algorithm, together with the function that we have seen in the course, to solve the DLP in $\mathbb{F}_p^*$. Does it run in polynomial, subexponential, or exponential time?

4. (a) (1p) Does the solution set to every equation

$$y^2 = x^3 + ax + b$$

(together with the point at infinity) give rise to an elliptic curve?

(b) (2p) The formulas used for adding points on an elliptic curve E work modulo any prime p and define a group structure on the points on this curve. However, modulo a composite number they do not always work. What can go wrong in this case?

(c) (4p) Suppose the addition of two points on an elliptic curve modulo some composite number N fails. How can this be used to factor N? Give a basic description of Lenstra's factorisation algorithm.

(d) (1p) For which choices of large N is Lenstra's factorization algorithm faster than the quadratic sieve?

(e) (2p) Lenstra's factorization algorithm is subexponential. Explain how this fact depends upon the distribution of B-smooth numbers.