Understanding Cryptography **Homework No. 6** **Due Date:**

1. Consider the following elliptic curve:
$$y^2 = x^3 + x + 6 \mod 11$$
Consider a DHKE protocol based on this elliptic curve with Alice's private key a = 6.
Alice receives Bob's public key $B = (5, 9)$. Calculate the session key for this protocol.

2. Consider the following elliptic curve:
$$y^2 = x^3 + 2x + 2 \mod 17$$
   a) Show that the condition $4a^3 + 27b^2 \neq 0 \mod p$ is fulfilled for this curve.
   b) Calculate $(2,7) + (5,2)$ with only a packet calculator.
   c) Verify Hasse's theorem for this curve.
   d) Describe why all elements are primitive elements?

3. Given an RSA signature scheme with the public key ($n = 9797, e = 131$), show how Oscar can perform an existential forgery attack by providing an example of such for the parameters of the RSA digital signature scheme.

4. Consider an Elgamal signature scheme with $p = 31$, $\alpha = 3$ and $\beta = 6$. You receive the message $x = 10$ twice with two signatures $(17,5)$ and $(13,5)$.
   a) Which one of these signatures is valid?
   b) How many valid signatures are there for each message x and the specific parameters chosen above?

5. Birth-date and the collision challenge!
   a) What is the minimum number of students in a class needed to have at least two students with the same birth-date with probability more than 1/2?
   b) If a year has N days and the number of students is K, find the probability of having at least two students with the same birth-date as a function of K and N.
   c) If we want to observe collision in a hash function with outputs of size n bits wit probability more than 1/2, how many random messages do we need?
   (hint: You can use the inequality $1 - x \leq e^{-x}, \quad x > 0$)

6. We consider three different hash functions which produce outputs of lengths 64, 128 and 160 bit. After how many random inputs do we have a probability of $\varepsilon = 0.5$ for a collision? After how many random inputs do we have a probability of $\varepsilon = 0.1$ for a collision?