Homework, Lecture 7

Problem A. Consider an elliptic curve

$$E_p = \left\{(x,y) : y^2 = x^3 + 7\right\} \bmod p$$

where $p = 127 = 2^7 - 1$ is the fourth Mersenne prime. How many integer points are on the elliptic curve. Compare your answer with Hasse's estimate. Prove that the point $\alpha = (19, 32)$ belongs to E_p and construct a sequence of $\beta_n = n\alpha$, $n = 1, ..., 100$. Explain in your own words whether this sequence is suitable for encryption purposes, and is so, how.

Problem B. Use MD5 algorithm as an inspiration and construct your own hash function $y = h(x)$, which maps an input x of any length into an output y of length 32 bits. Is it a good hash function? If not, can you produce a collision, i.e., find two distinct messages x, x' such that $h(x) = h(x')$.

Problem C. Design an efficient implementation of Random Oracle hash function of your own with 32 bit long output. Can you produce a collision, i.e., find two distinct messages x, x' such that $h(x) = h(x')$.

Problem D. Explain how a good hash function can be used to protect users' passwords. How would you try to break it? What is a dictionary attack?

Problem E. Use function from Problem B and try to solve a cryptographic puzzle, i.e., fund a sequence $x_1, ..., x_2$ such that $y_n = h(x_n)$ starts with n zeros.