Cryptography in Networking, Exercises 5 (October 12, 2017)

1) For the Diffie-Hellman key exchange protocol, Alice and Bob have selected to use public parameters $p = 41$ and $g = 7$. Check first that $g$ is indeed a generator. Compute the messages sent by both parties when Alice has chosen $a = 13$ and Bob has chosen $b = 11$. Compute also the key $k$.

2) Let us consider an EL GAMAL cryptosystem with commonly known parameters $p = 41$ and $g = 7$. Encrypt the message $x = 29$ for Bob whose public key is $13$. Please, use the random $b = 15$ in the process. Verify the result by decrypting the cryptotext with Bob’s private key $9$.

3) In the EL GAMAL signature system we have public parameters $p = 173$ and $g = 7$. Alice has signed the message $m_1$ that has the hash $h(m_1) = 77$ with $(59, 26)$ and another message $m_2$ that has hash $h(m_2) = 116$ with $(59, 153)$. Break Alice’s secret key. What is the learning from this?

4) Show that the equation $y^2 = x^3 + x$ defines an elliptic curve over $\mathbb{F}_7$. Find all points on the curve, then find one generator for the group of points and show how all other points can be represented as multiples of the generator point.

5) Calculate $P_{12} + P_{11}$ and $2P_3$ in the (lecture slide) example elliptic curve over the binary field $\mathbb{F}_{16}$.

6) Let us use the same curve group as in previous exercise for a toy example of the ECDH key exchange. The generator point is $G = P_3$. Find messages $X$ and $Y$ when $A$ has chosen $a = 4$ and $B$ has chosen $b = 3$. What is the shared secret?