Identification Systems

Exercises 1

Piotr Syga

March 9, 2021

1. Show the relationship between Diffie-Hellman protocol and Discrete Logarithm.
2. Show that Diffie-Hellman protocol is vulnerable against man in the middle attacks.
3. Propose a fix to DH protocol that allows MitM resistance, think of various solutions.
4. Show that the Diffie-Hellman protocol in $\mathbb{Z}_p^*$ between more than 2 users requires multiple rounds.
5. Show that there exists a single-round multi-party DH-protocol using pairings.
6. Consider Elliptic Curve $y^2 = x^3 + x + 3$ over $GF(7)$. Find all the points on the curve. Find the line between $P = (4, 1)$ and $Q = (6, 1)$. Find third point on the line and $P + Q$. Find the generator of the group. Find k such that $Q = kP$.
7. Recall the rules of adding two points on Elliptic Curves.
8. Transform the rule for adding $P \neq Q$ so that it holds for almost all points $P = Q$, name those points that should be treated differently.
9. Based on 'quick exponent by squaring' propose an algorithm for fast multiplication of point P by a constant k.
10. Using programming language of your choice (and selected modules/libraries) implement a module for Elliptic Curve operations and verify the proposed addition, substraction and multiplication algorithms. Find the time complexity (both the number of rounds and the time passed) for multiplication by a n-bit constant. Does it vary depending on the EC selected?
11. Propose a procedure that given two points P and kP finds k. Estimate the time complexity of the procedure, verify the influence of the length of k and the number of the points on the curve.

12. The curve $y^2 = x^3 + x + 24$ over F_{541} has 539 points. Plot the curve using your module. For $P = (423, 398)$ and $Q = (111, 58)$ find: $R = P + Q$, $T = P - Q$ and $S = 2P$. Solve the discrete logarithm problem $P = kQ$.

13. Recall the definition of ergodic Markov chains.

14. Recall coupling technique for Markov chains along with the Coupling Lemma and mixing time bound.

15. Let ID be a bit string of length $2n$ and let us, during each round, select n of the bits and reverse them, i.e., $b'_i = 1 - b_i$. Using coupling technique estimate the mixing time. Use Shoup's sequence of games to show that given $k < 2^{2n}$ initial IDs, after some time t', the transformed IDs are indistinguishable form random sequences. Find t' and compare it with the mixing time.