Cryptography, exercise sheet 5 for 1 Oct 2024

1. This is a continuation of exercise 4 from sheet 4, also matching the slides I showed in the lecture on Sep 26.

   Let $p = 1000003$. The elliptic curve $E : y^2 = x^3 - x$ over $\mathbb{F}_p$ has $1000004 = 2^2 \cdot 53^2 \cdot 89$ points. $P = (101384, 614510)$ is a point of order $2 \cdot 53^2 \cdot 89$ and $P_A = aP = (670366, 740819)$ is a multiple of P.

   In this exercise you will compute a_1, a_2, a_3, a_4 (from the slides) and solve the DLP.

   (a) Compute $a_2 \equiv a \bmod 2$ by solving the DLP in the order-2 subgroup.

   (b) Use the BSGS algorithm to solve the 2 DLPs in the order-53 subgroup to get a_2 and a_3. Make sure to update P_A before solving the second one – and do not overwrite your original P_A.

   (c) Solve the DLP in the size-89 subgroup. Feel free to use a for loop in Sage to solve this or the built in Sage funcction, but make sure to compute S and R, the new base and target.

   (d) Use the Chinese remainder theorem to compute a. Test your solution.

2. Let point P have order 411672 and point P_A be a multiple of P. Explain how to compute the DLP of P_A base P using the Pohlig-Hellman attack and estimate the number of steps needed.

3. This exercise is to be solved by hand, do not use a computer algebra system for the exponentiations or the CRT calculation.
   Compute $15^{24} \bmod 72$ using the Chinese Remainder Theorem with calculations modulo 8 and modulo 9. Remember to reduce the exponents and the base in the CRT calculation and take a moment to think what moduli to use and to check the conditions.
   In case this is not obvious $72 = 2^3 \cdot 3^2$, so this is not an RSA number and you need to use (and understand) the Euler-phi function and when you can reduce exponents.
   See RSA-II for how CRT is used for RSA moduli.

4. Perform the full RSA key generation for CRT-RSA for $p = 10007$, $q = 10427$, and $e = 65537 = 2^{16} + 1$.

5. Decrypt ciphertext $c = 4845315$ sent to the public key in the previous exercise. Use the CRT method to recover the message.