(1) Alice and Bob agree to use \((p, g) = (1373, 2)\) for ElGamal.

(a) First, Alice will send a message to Bob. So he picks a private key \(\rho_b = 716\) and computes the public key \(r_b = 2^{716} \equiv 469\); Alice chooses an ephemeral key \(\sigma_a = 877\) and message \(m_a = 583\). What is the ciphertext that Alice sends to Bob?

(b) Now they switch roles. Alice chooses a private key \(\rho_a = 299\); what is her public key \(r_a\)? Bob encrypts a message using \(r_a\) and sends Alice the ciphertext \((c_1, c_2) = (661, 1325)\). Decrypt the message.

(c) Finally, Bob chooses a new private key and publishes the associated public key \(B = 893\). Alice encrypts a message using this public key and sends the ciphertext \((c_1, c_2) = (693, 793)\) to Bob. You intercept the transmission. Decrypt the message by solving the appropriate discrete log problem.

(2) Show that (a) \(5 + 6x^2 - 37x^5 = \mathcal{O}(x^5)\) and (b) \((\log k)^{375} = \mathcal{O}(k^{0.001})\).

(3) Use babystep-giantstep to solve the following discrete log problems. (Do the first one on paper. Try writing a program in PARI for (b) and (c), and if possible attach a printout.)

(a) \(11^x \equiv 21 \pmod{71}\)

(b) \(156^x \equiv 116 \pmod{593}\)

(c) \(650^x \equiv 2213 \pmod{3571}\)

(4) Write out your own proof that the Pohlig-Hellman algorithm works in the particular case that \(p - 1 = q_1 \cdot q_2\) is a product of two distinct primes. (This needn’t be long – half a page or so.)

(5) Use Pohlig-Hellman to solve the discrete log problem \(7^x \equiv 166 \pmod{433}\).

(6) Artin conjectured that the number of primes \(p \leq x\) such that 2 is a primitive root mod \(p\) is asymptotic to \(C \pi(x)\) for some constant \(C\). (Recall it is still not even proved if there are infinitely many \(p\) having 2 as primitive root.) Using PARI, make an educated guess as to what “Artin’s constant” \(C\) should be, to a few decimal places of accuracy. Explain your reasoning. (Of course, don’t try to prove that your guess is correct.)