Cryptography, exercise sheet 6 for 08 Oct 2024

You can use Sage or other computer-algebra systems for the computations in the specified algorithms but do not just call `factor`.

1. You learn that I sent ciphertext $c = 146825627869398061752588778309232041959671041598158622$ to a user with RSA public key $(e, n) = (3, 529774210762246675161318616746995617835565246251635147)$ and that this was the result of a form which sends a stereotyped message `myfavoritenumberis____` in base 36, where the empty spaces indicate 6 unknown characters. Use LLL to recover those 6 characters.
   Note that you are not guaranteed to succeed with the first output of LLL. Also note that you can (and should) check your solution.

   Note: See RSA XI for Sage code regarding stereotyped messages.

2. Use Pollard's rho method for factorization to find a factor of 27887. Use starting point $\rho_0 = 17$, iteration function $\rho_{i+1} = \rho_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(\prod_{i=1}^{z}(\rho_{2i} - \rho_i), 27887)$ until a non-trivial gcd is found. Deviating from the proper method, do the gcd computations after each i, so skip the product over z. Document the intermediate steps in a table, with one row for ρ_i, one for ρ_{2i}, and one for their gcd.

3. Use the $p - 1$ method to factor 27887 with basis $a = 2$ and exponent $s = \mathrm{lcm}(1, 2, 3, 4, 5, \ldots, 11)$.
   Explain why the method worked.
   Note: to answer the latter question you need to look at the factors of $p - 1$ and $q - 1$ and argue about how likely it was that you would pick an a so that these two primes split when computing $\gcd(a^s - 1, 27887)$.