

Cryptography, exercise sheet 5 for 29 Sep 2026

1. Perform the full RSA key generation for CRT-RSA for $p = 10007$, $q = 10427$, and $e = 65537 = 2^{16} + 1$.
2. Decrypt ciphertext $c = 4845315$ sent to the public key in the previous exercise. Use the CRT method to recover the message.
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. 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.
5. Use the $p - 1$ method to factor 27887 with basis $a = 2$ and exponent $s = \text{lcm}(1, 2, 3, 4, 5, \dots, 11)$.
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 $\gcd(a^s - 1, 27887)$.