

Cryptography, exercise sheet 6 for 06 Oct 2026

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

For the exercises on Coppersmith's method, investigate why the method worked using the theorem by Howgrave-Graham. You can find the exact statement and the code snippets on the [slides](#) that Tanja showed.

1. This exercise is copied from last week.

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 $\gcd(a^s - 1, 27887)$.

2. This exercise is about factoring with known bits of p . Alice uses RSA key $(n, e) = (676283665767010291339720070207048493311188820369060388664881657648635309, 65537)$ and you know that factors p and q have 120 bits. You also learn the top part of p , more precisely $p = a + r$ for $r < 2^{38}$ and $a = 596179186328948214111920714820878336$.

Use Coppersmith's method to factor n .

3. This exercise is about factoring with known bits of p . Alice uses RSA key $(n, e) = (5116590796535407135368494745739989640361383246886672243281912124639, 65537)$ and you know that factors p and q have 112 bits. You also learn the bottom part of p , more precisely $p = a + r2^{76}$ for $r < 2^{36}$ and $a = 69521552185397560397005$.

Figure out how to use Coppersmith's method to factor n .

Hint: Note that the entries in the matrix would be way too big if you kept the 2 there. To get rid of the large power of 2, note that it is coprime to n .

4. 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.