Theorem 9.3 (Coppersmith, 1997). *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d and let N be a positive integer. If there is a solution of the congruence $f(x_0) \equiv 0 \pmod{N}$, which satisfies the inequality $|x_0| \leq N^{1/d-\epsilon}$, then there is an algorithm which can find x_0, and whose complexity is polynomial in $\ln N$ and $1/\epsilon$ (for fixed d).*

9.6 Exercises

1. By using "brute force" attack, i.e. by examining all 26 possible keys, decrypt the ciphertext

   SGZNKSGZOIY

   obtained by Caesar's cipher.

2. Encrypt the plaintext

   NUMBERTHEORY

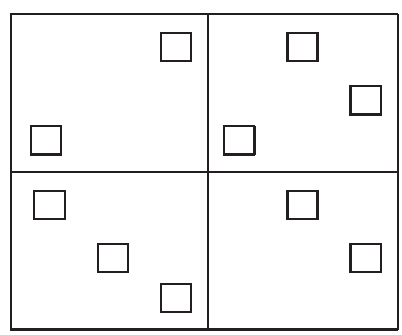
   by using Vigenère's cipher with the key $2, 24, 15, 7, 4, 17$.

3. Encrypt the plaintext

   INTERNATIONALIZATION

   by columnar transposition with the key (the order of rows) 4 3 1 2 5.

4. In the holes at 6×6 grid from the figure, write the plaintext SEVEN TANKS and then try to fill out the remaining 26 positions in the square in such a manner that you obtain at least a somewhat meaningful message within which the plaintext will be hidden.



5. Let $P(m)$ be the number of ways in which m pairs of letters can be chosen among 26 letters. For which $m \in \{1, 2, \ldots, 13\}$ is number $P(m)$ the largest?

6. Factorize the following positive integers:

$$999\,919, \quad 3\,999\,991, \quad 80\,999\,999, \quad 224\,999\,711.$$

7. Factorize $n = 737419$ if it is known that n is the product of two "close" prime numbers.

8. In the RSA cryptosystem with the public key (n, e), where $n = 86267 = 281 \cdot 307$ and $e = 65537$, encrypt the plaintext

$$x = 1245.$$

Determine the private key d.

9. Choose two distinct four-digit prime numbers p and q. Let $n = p \cdot q$. Choose a five-digit number e which is relatively prime to $\varphi(n)$. Encrypt the plaintext

$$x = 123417$$

by using the RSA cryptosystem with the public key (n, e). Determine the corresponding private key d.

10. A plaintext in English is encrypted by using cryptosystem RSA whose public key is $(n, e) = (30967, 17)$. First, the corresponding numerical values: A $= 0$, B $= 1$, C $= 2$, $\ldots$, Y $= 24$, Z $= 25$ are associated to the letters. Then three by three adjacent letters of the plaintext are "coded" as elements of $\mathbb{Z}/n\mathbb{Z}$, as illustrated in these examples:

$$\text{ONE} = 14{\cdot}26^2{+}13{\cdot}26{+}4 = 9806, \quad \text{TWO} = 19{\cdot}26^2{+}22{\cdot}26{+}14 = 13430.$$

Finally, the obtained elements of $\mathbb{Z}/n\mathbb{Z}$ are encrypted by using the RSA cryptosystem with the above parameters n and e.

Factorize the number n (it is known that the product of two "close" prime numbers) and decrypt the ciphertext

$$7\,663, \quad 13\,134, \quad 12\,274, \quad 11\,615.$$

11. Explain reasons why it is not a good idea to use the RSA cryptosystem in such a manner that a letter by letter of the plaintext is encrypted (after replacing A $= 0$, B $= 1, \ldots,$ Z $= 25$). How can messages encrypted in this way be easily "broken", even in the case where modulus n is a very large number which we do not know how to factorize? This is an example of protocol failure, of an otherwise secure cryptosystem.

12. Let n be a positive integer which is the product of two prime numbers p and q. Show that from knowing numbers n and $\varphi(n)$ it is possible to calculate numbers p and q. Illustrate the method on the example $n = 30700619$ and $\varphi(n) = 30689496$.

13. Let $(n, e) = (32311427, 22100011)$ be the public RSA key. It is known that the private exponent d satisfies the inequality $d < \frac{1}{3}\sqrt[4]{n}$. Determine d by using Wiener's attack.

14. Prove that in the rebalanced RSA, the plaintext x can be calculated through the formula

$$x = x_p + p((x_q - x_p)p^{-1} \bmod q).$$

15. Alice sent an identical message m to several agents. Eve interfered ciphertexts c_1, c_2, c_3 for three agents whose public keys are n_1, n_2 and n_3. It is known that Alice and agents use the RSA cryptosystem with the public exponent $e = 3$. For given

$$\begin{aligned} n_1 &= 407, \quad & c_1 &= 356, \\ n_2 &= 533, \quad & c_2 &= 281, \\ n_3 &= 551, \quad & c_3 &= 468, \end{aligned}$$

show how Eve can determine the message m (without knowing factorizations of moduli n_1, n_2, n_3).

16. Apply Coppersmith's method to the polynomial $f(x) = x^2 + ax + b$ with $m = 1$. For N large enough, the method finds a solution x_0 of the congruence $f(x_0) \equiv 0 \pmod{N}$ if $|x_0| \leq N^\delta$. Determine the exponent δ.