Chapter 7

Lattices and Cryptography

The security of all of the public key cryptosystems that we have previously studied has been based, either directly or indirectly, on either the difficulty of factoring large numbers or the difficulty of finding discrete logarithms in a finite group. In this chapter we investigate a new type of hard problem arising in the theory of lattices that can be used as the basis for a public key cryptosystem. Lattice-based cryptosystems offer several potential advantages over earlier systems, including faster encryption/decryption and so-called quantum resistance. The latter means that at present there are no known quantum algorithms to rapidly solve hard lattice problems; see Sect. 8.11. Further, we will see that the theory of lattices has applications in cryptography beyond simply providing a new source of hard problems.

Recall that a vector space V over the real numbers $\mathbb{R}$ is a set of vectors, where two vectors can be added together and a vector can be multiplied by a real number. A lattice is similar to a vector space, except that we are restricted to multiplying the vectors in a lattice by integers. This seemingly minor restriction leads to many interesting and subtle questions. Since the subject of lattices can appear somewhat abstruse and removed from the everyday reality of cryptography, we begin this chapter with two motivating examples in which lattices are not mentioned, but where they are lurking in the background, waiting to be used for cryptanalysis. We then review the theory of vector spaces in Sect. 7.3 and formally introduce lattices in Sect. 7.4.

7.1 A Congruential Public Key Cryptosystem

In this section we describe a toy model of a real public key cryptosystem. This version turns out to have an unexpected connection with lattices of dimension 2, and hence a fatal vulnerability, since the dimension is so low. However,

J. Hoffstein et al., *An Introduction to Mathematical Cryptography*,
Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4939-1711-2_7

it is instructive as an example of how lattices may appear in cryptanalysis even when the underlying hard problem appears to have nothing to do with lattices. Further, it provides a lowest-dimensional introduction to the NTRU public key cryptosystem, which will be described in Sect. 7.10.

Alice begins by choosing a large positive integer q, which is a public parameter, and two other secret positive integers f and g satisfying

$$f < \sqrt{q/2}, \qquad \sqrt{q/4} < g < \sqrt{q/2}, \qquad \text{and} \qquad \gcd(f, qg) = 1.$$

She then computes the quantity

$$h \equiv f^{-1}g \pmod{q} \qquad \text{with } 0 < h < q.$$

Notice that f and g are small compared to q, since they are $\mathcal{O}(\sqrt{q})$, while the quantity h will generally be $\mathcal{O}(q)$, which is considerably larger. Alice's private key is the pair of small integers f and g and her public key is the large integer h.

In order to send a message, Bob chooses a plaintext m and a random integer r (a random element) satisfying the inequalities

$$0 < m < \sqrt{q/4} \qquad \text{and} \qquad 0 < r < \sqrt{q/2}.$$

He computes the ciphertext

$$e \equiv rh + m \pmod{q} \qquad \text{with } 0 < e < q$$

and sends it to Alice.

Alice decrypts the message by first computing

$$a \equiv fe \pmod{q} \qquad \text{with } 0 < a < q,$$

and then computing

$$b \equiv f^{-1}a \pmod{g} \qquad \text{with } 0 < b < g. \tag{7.1}$$

Note that f^{-1} in (7.1) is the inverse of f modulo g.

We now verify that $b = m$, which will show that Alice has recovered Bob's plaintext. We first observe that the quantity a satisfies

$$a \equiv fe \equiv f(rh + m) \equiv frf^{-1}g + fm \equiv rg + fm \pmod{q}.$$

The size restrictions on f, g, r, m imply that the integer $rg + fm$ is small,

$$rg + fm < \sqrt{\frac{q}{2}}\sqrt{\frac{q}{2}} + \sqrt{\frac{q}{2}}\sqrt{\frac{q}{4}} < q.$$

Thus when Alice computes $a \equiv fe \pmod{q}$ with $0 < a < q$, she gets the exact value

Alice	Bob
Key Creation	
Choose a large integer modulus q. Choose secret integers f and g with $f < \sqrt{q/2}$, $\sqrt{q/4} < g < \sqrt{q/2}$, and $\gcd(f, qg) = 1$. Compute $h \equiv f^{-1}g \pmod{q}$. Publish the public key (q, h).	
Encryption	
	Choose plaintext m with $m < \sqrt{q/4}$. Use Alice's public key (q, h) to compute $e \equiv rh + m \pmod{q}$. Send ciphertext e to Alice.
Decryption	
Compute $a \equiv fe \pmod{q}$ with $0 < a < q$. Compute $b \equiv f^{-1}a \pmod{g}$ with $0 < b < g$. Then b is the plaintext m.	

Table 7.1: A congruential public key cryptosystem

$$a = rg + fm. \tag{7.2}$$

This is the key point: the formula (7.2) is an equality of integers and not merely a congruence modulo q. Finally Alice computes

$$b \equiv f^{-1}a \equiv f^{-1}(rg + fm) \equiv f^{-1}fm \equiv m \pmod{g} \qquad \text{with } 0 < b < g.$$

Since $m < \sqrt{q/4} < g$, it follows that $b = m$. The congruential cryptosystem is summarized in Table 7.1.

Example 7.1. Alice chooses

$$q = 122430513841, \quad f = 231231, \quad \text{and} \quad g = 195698.$$

Here $f \approx 0.66\sqrt{q}$ and $g \approx 0.56\sqrt{q}$ are allowable values. Alice computes

$$f^{-1} \equiv 49194372303 \pmod{q} \quad \text{and} \quad h \equiv f^{-1}g \equiv 39245579300 \pmod{q}.$$

Alice's public key is the pair $(q, h) = (122430513841, 39245579300)$.

Bob decides to send Alice the plaintext $m = 123456$ using the random value $r = 101010$. He uses Alice's public key to compute the ciphertext

$$e \equiv rh + m \equiv 18357558717 \pmod{q},$$

which he sends to Alice.

In order to decrypt e, Alice first uses her secret value f to compute

$$a \equiv fe \equiv 48314309316 \pmod{q}.$$

(Note that $a = 48314309316 < 122430513841 = q$.) She then uses the value $f^{-1} \equiv 193495 \pmod{g}$ to compute

$$f^{-1}a \equiv 193495 \cdot 48314309316 \equiv 123456 \pmod{g},$$

and, as predicted by the theory, this is Bob's plaintext m.

How might Eve attack this system? She might try doing a brute-force search through all possible private keys or through all possible plaintexts, but this takes $\mathcal{O}(q)$ operations. Let's consider in more detail Eve's task if she tries to find the private key (f, g) from the known public key (q, h). It is not hard to see that if Eve can find any pair of positive integers F and G satisfying

$$Fh \equiv G \pmod{q} \quad \text{and} \quad F = \mathcal{O}(\sqrt{q}) \quad \text{and} \quad G = \mathcal{O}(\sqrt{q}), \tag{7.3}$$

then (F, G) is likely to serve as a decryption key. Rewriting the congruence (7.3) as $Fh = G + qR$, we reformulate Eve's task as that of finding a pair of comparatively small integers (F, G) with the property that

$$\begin{array}{c}\text{unknown integers}\\ \overset{\downarrow}{F}\,\underbrace{(1,h)}_{\uparrow} - \overset{\downarrow}{R}\,\underbrace{(0,q)}_{\uparrow} = \overbrace{(F,G)}^{\substack{\text{unknown}\\ \text{small}\\ \text{vector}}}.\\ \text{known vectors}\end{array}$$

Thus Eve knows two vectors $\boldsymbol{v}_1 = (1, h)$ and $\boldsymbol{v}_2 = (0, q)$, each of which has length $\mathcal{O}(q)$, and she wants to find a linear combination $\boldsymbol{w} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2$ such that $\boldsymbol{w}$ has length $\mathcal{O}(\sqrt{q}\,)$, but keep in mind that the coefficients a_1 and a_2 are required to be integers. Thus Eve needs to find a short nonzero vector in the set of vectors

$$L = \{a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 : a_1, a_2 \in \mathbb{Z}\}.$$

This set L is an example of a two-dimensional lattice. Notice that it looks sort of like a two-dimensional vector space with basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$, except that we are allowed to take only integer linear combinations of $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$.

Unfortunately for Bob and Alice, there is an extremely rapid method for finding short vectors in two-dimensional lattices. This method, which is due to Gauss, is described in Sect. 7.13.1 and used to break the congruential cryptosystem in Sect. 7.14.1.