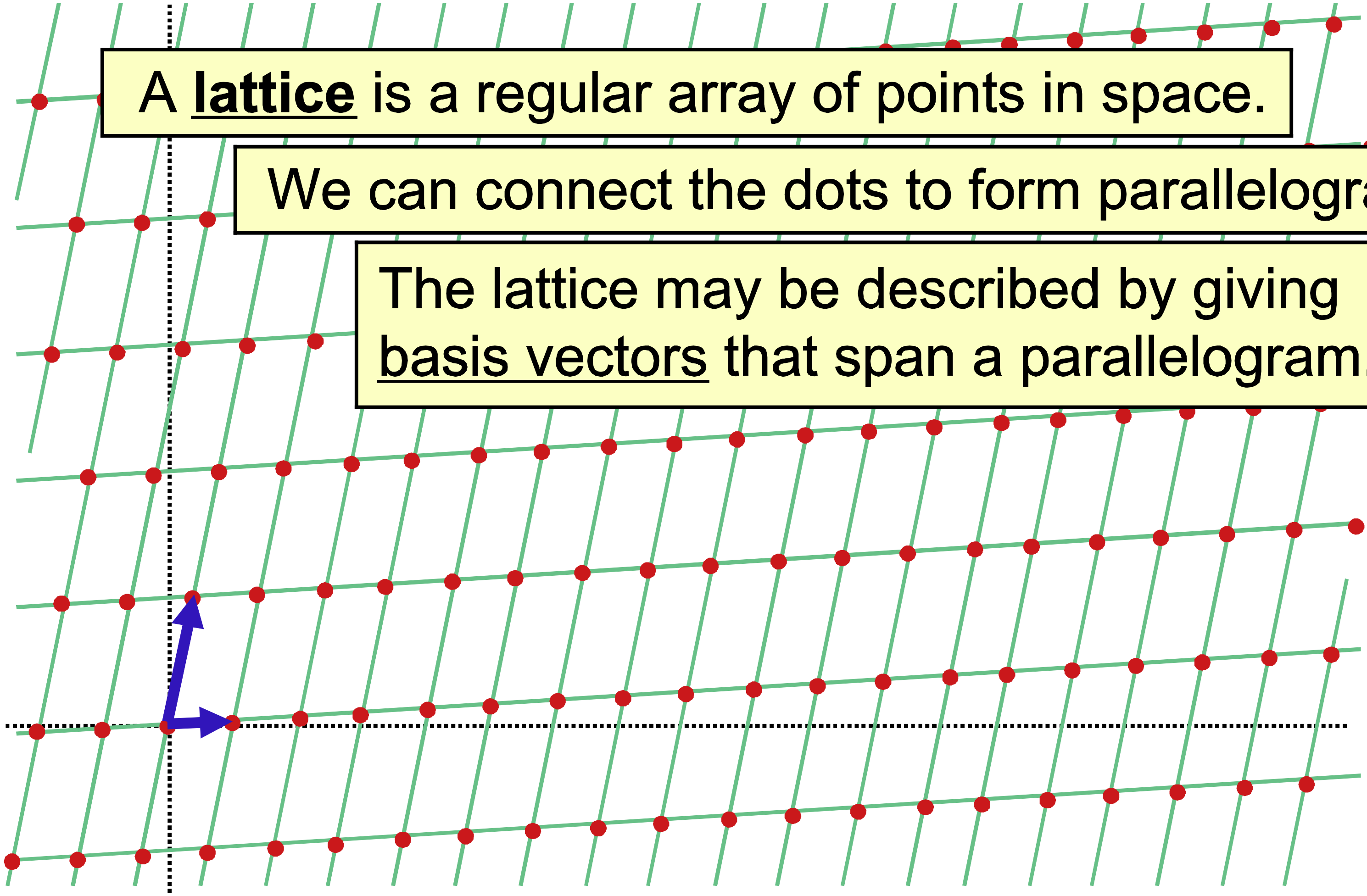
Chapter 70

Advanced Data Encryption

What is a Lattice?



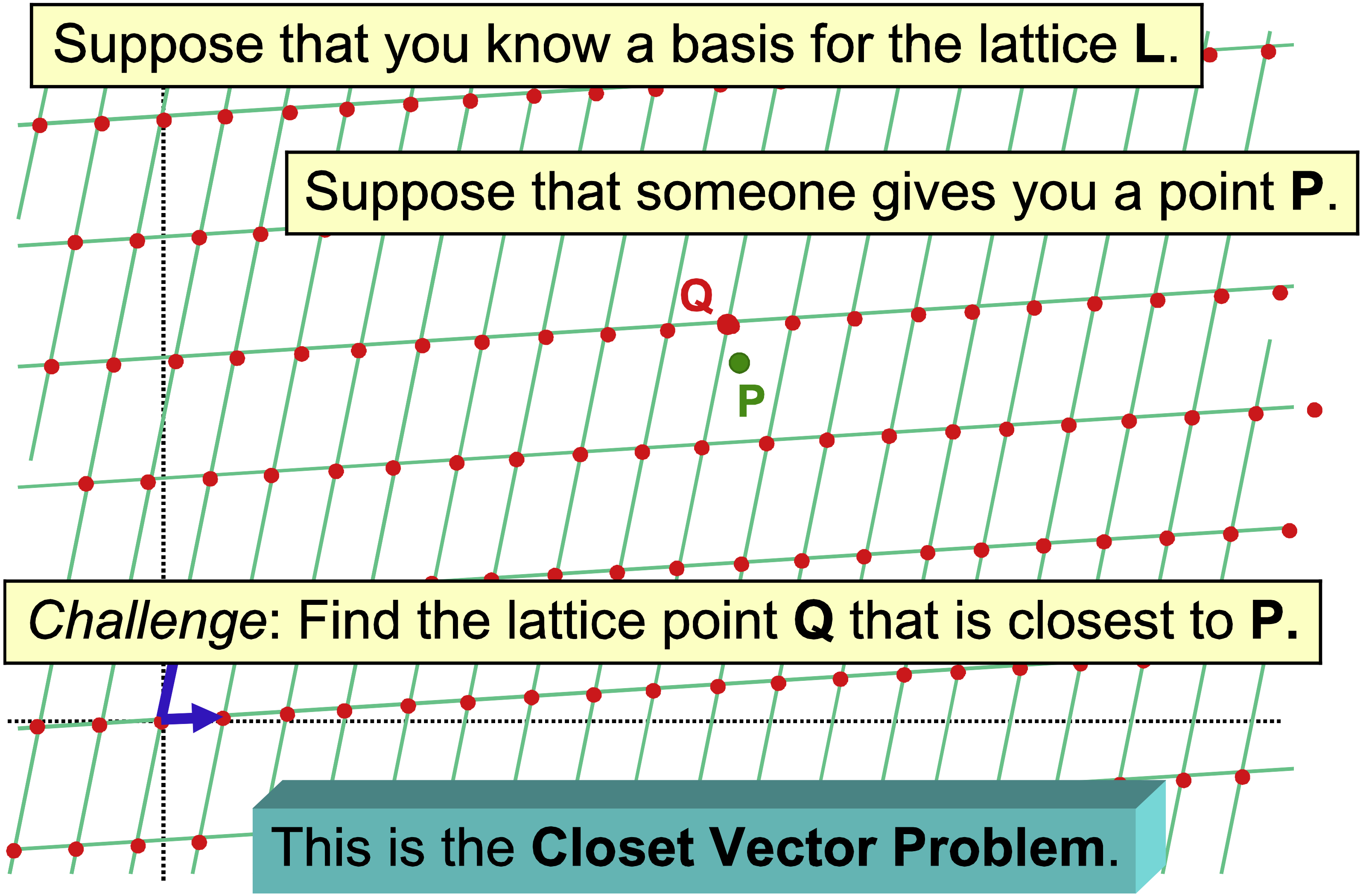
A **lattice** is a regular array of points in space.

We can connect the dots to form parallelograms.

The lattice may be described by giving basis vectors that span a parallelogram.

f70-01-9780123943972

What is the Closest Vector Problem?



Suppose that you know a basis for the lattice **L**.

Suppose that someone gives you a point **P**.

Challenge: Find the lattice point **Q** that is closest to **P.**

This is the **Closet Vector Problem.**

f70-02-9780123943972

Why Is That A Hard Problem?

For lattices in the plane, you’re right, it’s very easy. It’s not even very hard in dimension 3, or 4, or 5. However, the Closest Vector Problem is **very hard** in high dimension, say in dimension 500.

f70-03-9780123943972