Shor’s quantum algorithm can be used to factor large integers efficiently in a quantum computer. This is currently believed to be a hard problem for ordinary computers. Building a quantum computer is currently difficult and a research subject at many universities and companies. This toolbox provides an interactive experience where students gradually work their way to an understanding of Shor’s algorithm.

**Kit contents**

- $S$: x1
- $H$: x4
- $\oplus$: x6
- $\oplus$: x2
- $\times$: x4
- $\times$: x5

Plus cables and power supply.

**Contact**

sales@phasespacecomputing.com

---

**The Algorithm**

Shor’s algorithm uses quantum phase estimation to find the order of the modular exponentiation function, and this can be used to find a factor in the modulus. Shor’s algorithm scales with the cube of the number of bits needed to express the modulus, while no efficient classical algorithm is known. This kit can be used to factor 15, the first nontrivial example of factoring a composite integer.

**Technology**

This toolbox contains a modular kit of electronic circuit boards that approximate the behavior of quantum gates, a patent pending technology that has been developed at Linköping University, Sweden.