Quantum cryptography is the science of exploiting fundamental effects and principles of quantum physics, in the development of cryptographic protocols that are secure against the most malicious adversaries (hackers) allowed by the laws of physics, the so-called "quantum adversaries". In analogy to conventional cryptography, one may define quantum cryptographic primitives, with different security objectives. One of these primitives, the so-called quantum key-distribution, is currently the most advanced field of quantum technologies, and is considered to be a cornerstone for a global quantum internet. The main aim of this pedagogical talk is to introduce a non-specialized audience to the world of quantum cryptography. I will discuss why quantum cryptography is so important for the future, and what are the main underlying principles and techniques. I will conclude with a brief review of the current status of the field and an outline of the main challenges.