In the present work we study provable security in the random oracle model and the standard model using the OAEP cryptosystem as an example. We begin with general introduction to public-key cryptography. In the next chapter we trace the evolution of RSA-OAEP cryptosystem security proofs in the random oracle model from the original controversial proof of security from 1994 to the correct and technically challenging one from 2004. The third chapter is dedicated to the selected problematic aspects of RSA-OAEP practical security. The goal of the extensive fourth chapter is to present some of the most recent results regarding the security of RSA-OAEP in the standard model. The first result from 2009 shows the fundamental impossibility of security proof construction in the sense of CCA2. The result from 2006, despite being positive (weak non-malleability of fully-instantiated OAEP), is of an arguable significance. In the end we mention some comments on the state-of-the-art provable security of RSA-OAEP.