The aim of this work is to introduce the reader to the protocol TLS and a few selected attacks against the protocol. In the first part we will define the necessary cryptographic definitions used in the following chapters. In the second part we will briefly talk about the history of procotols TLS and SSL and then we will closely look into how they work. The last part is about the analysis of the chosen cryptographically interesting attacks (Padding oracle on CBC mode, POODLE, BEAST and CRIME) against protocols TLS and SSL.