Cílem této práce je seznámit čtenáře s protokolem TLS (dříve SSL) a vybranými útoky na tento protokol. V první části práce si zavedeme nezbytné kryptografické definice použité v následujících kapitolách. V druhé části si stručně představíme historii protokolů TLS a SSL, a poté se blíže podíváme na to, jak fungují. Poslední část se týká rozboru vybraných kryptograficky zajímavých útoků (Padding oracle na CBC mód, POODLE, BEAST a CRIME) na protokoly TLS a SSL.