Abstrakt: Diffie-Hellmanov (DH) problém je problém, o ktorom sa predpokladá, že je ťažký. Preto sa naň redukuje bezpečnosť mnohých kryptografických systémov. V tejto práci sa zoznámime s novou variantou DH problému — so zdvojeným DH problémom. Vytvoríme si metódu, ktorá nám dovolí simulovať rozhodovacie orákulum bez znalosti príslušného diskrétneho logaritmu daných prvkov. Ukážeme si zdvojené ElGamalovo šifrovanie a jeho bezpečnosť v modele náhodného orákula. ElGamalovo šifrovanie je bezpečné pri útoku vybraním zašifrovaného textu za predpokladu, že je proti tomuto útoku bezpečná aj príslušná symetrická šifra. Dokážeme si, že zdvojený DH protokol na neinteraktívnu výmenu kľúča je v modele náhodného orákula bezpečný proti aktívnym útokom. V oboch prípadoch stačí predpokladať platnosť DH predpokladu.