V této diplomové práci se zabýváme detailním vysvětlením pojmu CCZ-ekvivalence spolu s analýzou některých speciálních tvarů ekvivalenčních matic. Také se věnujeme zkoumání diferenciální kryptoanalýzy vyšších řádů a její zobecněné verze. Pro lepší ilustraci této metody představujeme několik útoků na jednoduchou pětirundovou Feistelovu šifru, dva z útoků jsou naše vlastní. Ty nejdůležitější útoky jsme implementovali a výsledky těchto experimentů jsou k nalezení v textu. Dále v práci zkoumáme, jak využít rozkladu $F = F_2 \circ F_1^{-1}$ (kde F_1 i F_2 jsou permutace) pro konstrukci zobecněného útoku vyšších řádů na blokovou šifru s S-boxem F. Tato konstrukce může být využita pro hledání útoku na F s použitím CCZ-ekvivalence, což je obecně těžký problém. Výsledkem našeho zkoumání je pak věta, která představuje nutnou podmínku na stupeň funkce F pro existenci takového rozkladu.