Hašovací funkce jsou důležitým kryptografickým primitivem. V kryptografii se využívají k prokázání původu zprávy, k detekci změn ve zprávě a v některých autentizačních protokolech. Tato práce uvádí přehled některých nových generických útoků proti hašovacím funkcím. Podrobně popisuje útok na autentizační hašovací funkci COMP128 využívanou do roku 2002 v GSM síti. Práce dále poukazuje na možné nedostatky v návrhu nové autentizační funkce SQUASH navrhnuté pro využití na RFID čipu.