Hash functions are an important cryptographic primitive. They are used as message authentication codes, manipulation detection codes and in many cryptograhic protocols. This thesis gives an explanation of the recent generic attacks against hash functions. It also explains the attack against authentication hash function COMP128, which was being used til 2002 in GSM network. The thesis also discusses possible flaws in a new authentication hash function SQUASH designed for an RFID chip.