**Kratki opis sustava zaštite**

Sustav koristi AES simetričnu enkripciju (Cipher-Block Chaining varijantu). Kao ključ za enkriptiranje zaporki, koristi se funkcija derivacije ključa, koja prima nekoliko parametara. Vrijeno je za spomenuti parametar *salt* pomoću kojeg je osigurano da svaki put enkriptiran sadržaj bude drukčiji, čak i u slučaju kad se lozinka mijenja na istu, staru lozinku. Tad napadač ne može odrediti je li se lozinka uistinu promijenila ili nije. *Salt* se kreira generatorom slučajnih brojeva, a sastoji se od 16 bajtova. Sljedeće što funkciji derivacije ključa treba je nešto iz čega će derivirati ključ. U ovom slučaju je odabrano da to bude *master* lozinka, jer na taj način osiguravamo da ključ bude isti pri dekripciji.

Osiguran je i integritet lozinke i adrese, tj. napadač ne može zamijeniti dvije lozinke da korisnik ne bude obaviješten. AES (CBC) kao jedan od ulaznih parametara prima inicijalizacijski vektor (*iv)*. Ovdje hash funkcija (SHA256) adrese služi kao inicijalizacijski vektor, što omogućava integritet lozinke i adrese. Naime, pri dekriptiranju lozinke se također koristi *iv*, koji ukoliko ne bude isti kao u trenutku enkriptiranja, bit će nemoguće *otključati* lozinku za tu adresu. Ako napadač zamijeni lozinku jedne adrese s lozinkom neke druge adrese u bazi i korisnik pokuša dohvatiti lozinku za jednu od tih adresa, sustav će uhvatiti grešku i obavijestiti korisnika da mu je baza u opasnosti te da pod hitno osigura bazu.