Criptare autentificata pe criptovaluta.

Bejan Octavian Alexandru

April 2018

1 Introducere

Criptarea autentificata reprezinta o forma de criptare care asigura simultan confidentialitatea, integritatea si autenticitatea datelor.Aceasta reprezinta o componenta foarte importanta a criptografiei, si de aceea este foarte des utilizata in protocoalele de securitate. In aceasta lucrare de licenta vom vorbi despre aplicatii ale criptarii autentificate existente pana la ora actuala, cat si despre unele mai noi despre care inca nu se stiu prea multe detalii.

Vom incepe prin a discuta despre cele mai cunoscute protocoale de securitate ce utilizeaza criptarea autentificata, ca de exemplu: IPSec, SSL/TLS, SSH, Kerberos, iar mai apoi ne vom axa atentia asupra subiectului acestei lucrari de licenta, si anume criptomonedele si modul in care acestea utilizeaza criptarea autentificata pentru mentinerea datelor in siguranta.

Cuprins

2 Cuprins

2.1 Introducere

In acest capitol ne vom crea o imagine de ansamblu asupra tezei de licenta.Tot in acest capitol voi evidentia motivul pentru care am ales sa studiez mai in profunzime criptografia.

2.1.1 Istoria criptografiei

Criptografia reprezintă o ramură a matematicii care se ocupă cu securizarea informației precum și cu autentificarea și restricționarea accesului într-un sistem informatic.

Criptografia dateaza inca din timpuri, cand aceasta era utilizata pentru a comunica in secret, pentru a asigura confidentialitate mesajului transmis. In prezent, criptografia a inceput sa se extinda, astfel ca pe langa problemele de confidentialitate au inceput sa apara noi tehnici de verificare a integritatii unui mesaj, de autentificare a emitatorului cat si a receptorului, semnaturi electronice, precum si calcule securizate.

Cercetările academice desfășurate în domeniul criptografiei sunt relativ recente - au inceput abia la sfarsitul anilor '70 odata cu aparitia comunicarii wireless si a criptarii cu chei publice. De atunci criptografia a devenit o unealta folosita la scara larga in general in securitatea informatiei.

2.1.2 Motivatie

Am ales aceasta tema deoarece doresc sa dobandesc mai multe informatii din domeniul securitatii informatiei.

2.1.3 Structura tezei

In prima parte a tezei de licenta vom afla mai multe informatii despre ceea ce reprezinta criptarea, in special cea autentificata.

In a doua parte vom discuta despre cele mai cunoscute aplicatii ale criptarii autentificate in acest moment, iar mai apoi vom afla mai multe despre criptovaluta, subiectul principal al acestei lucrari.

2.2 Criptare autentificata

2.2.1 Criptarea autentificata

Criptarea autentificata reprezinta o forma de criptare care asigura simultan confidentialitatea, integritatea si autenticitatea datelor. Lipsa acestei forme de criptare a reprezentat o mare problema pentru criptosistemele ce se doreau a fi puse in practica.

2.2.2 Notatii si sintaxa

Un sistem de criptare este o structura ($\mathcal{P}$,$\mathcal{C}$,$\mathcal{K}$,$\mathcal{E}$,$\mathcal{D}$) unde:

$\mathcal{P}$ = {w | w $\in$ V *} este multimea "textelor clare", scrise peste un alfabet nevid V. (uzual V = {0, 1}).
$\mathcal{C}$ = {w | w $\in$ W* } este multimea "textelor criptate", scrise peste un alfabet nevid W. (uzual W = V)
$\mathcal{K}$ reprezinta multimea de elemente numite chei.
$\mathcal{E}$ = multimea algoritmilor de criptare.
$\mathcal{D}$ = multimea algoritmilor de decriptare.

Fie w $\in \mathcal{P}$ un mesaj in clar, k $\in \mathcal{K}$ o cheie, $e_k \in \mathcal{E}$ algoritmul de criptare, si $d_k \in \mathcal{D}$ algoritmul de decriptare, atunci:

$e_k : \mathcal{P} \rightarrow \mathcal{C}$, e_k(w) = c, c reprezinta rezultatul criptarii textului w cu cheia k utilizand algoritmul e

2.2.3 Scheme de criptare

In prezent exista mai multe scheme de criptare.