Criptare autentificata si criptomenede

Bejan Octavian Alexandru

April 2018

Facultatea de Informatica,
Universitatea Alexandru Ioan Cuza Iasi

Mic cuprins

1 Introducere **3**

2 Tehnologii utilizate **3**

3 Mic cuprins **4**
3.1 Introducere 4
3.1.1 Istoria criptografiei 4
3.1.2 Structura tezei 4
3.2 Criptare autentificata 5
3.2.1 Criptarea autentificata 5
3.2.2 Notatii si sintaxa 5
3.2.3 Scheme de criptare 5
3.2.4 Modul de operare 5
3.3 Noi aplicatii ale criptarii autentificate - Criptomonedele 6
3.3.1 Introducere 6
3.3.2 Utilizare 6
3.3.3 Confidentialitate 6
3.3.4 Integritatea 6
3.3.5 Schema de criptare si autentificare 6
3.3.6 Modul de operare 6
3.4 Aplicatii cunoscute la ora actuala 6
3.4.1 Bitcoint 6
3.4.2 Ethereum 6
3.5 Lucrare practica 7
3.5.1 Informatii generale 7
3.5.2 Aspecte importante 7
3.5.3 Cum subliniaza lucrarea ideea de criptare autentificata . . 7
3.6 Bibliografie 7

1 Introducere

De ce acest subiect? Am ales acest subiect deoarece doresc sa imi aprofundez cunostintele deja existente,dar si pentru ca vreau sa devin un specialist in domeniul securitatii informatiei.

De ce criptomonede? Deoarece reprezinta o tehnologie ce a starnit interesul in ultima perioada, si deoarece utilizeaza un numar relativ mare de operatiile criptarii autentificate.

2 Tehnologii utilizate

Ca limbaj de programare voi utilizate python 3.x deoarece sunt familiarizat cu acesta. In plus se gasesc destule tutoriale despre modul in care poti "programa" criptomonelede (atat bitcoins cat si etherium).

In limita timpul disponibil voi dori sa incerc sa utilizez un Raspberry Pi pentru a sublinia modul in care functioneaza un miner de criptomonede.

3 Mic cuprins

3.1 Introducere

3.1.1 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.

3.1.2 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 criptovaluta, subiectul principal al acestei lucrari, cat si despre cele mai cunoscute aplicatii ale criptarii autentificate in domeniul criptomonedelor.

3.2 Criptare autentificata

3.2.1 Criptarea autentificata

Definitie

Cand si de ce este folosita?

3.2.2 Notatii si sintaxa

Un sistem de criptare este o structura ($\mathcal{P}$,$\mathcal{C}$,$\mathcal{K}$,$\mathcal{E}$,$\mathcal{D}$). Explicatie fiecare componenta a sistemului.

3.2.3 Scheme de criptare

Encrypt-then-MAC (EtM)

Encrypt-and-MAC (E&M)

MAC-then-Encrypt (MtE)

3.2.4 Modul de operare

3.3 Noi aplicatii ale criptarii autentificate - Criptomonedele

3.3.1 Introducere

De unde provine termenul, si ce reprezinta.

3.3.2 Utilizare

Cand este folosita.

De cine este folosita.

De ce este folosita.

3.3.3 Confidentialitate

Ce reprezinta confidentialitatea?

Cum ofera criptomonedele confidentialitate?

3.3.4 Integritatea

Ce reprezinta integritatea?

Cum ofera criptomonedele confidentialitate?

3.3.5 Schema de criptare si autentificare

Explicatii pentru fiecare componenta.

3.3.6 Modul de operare

3.4 Aplicatii cunoscute la ora actuala

3.4.1 Bitcoint

Scurt istoric.

Ideea generala din spatele acestei monede.

3.4.2 Ethereum

Scurt istoric.

Ideea generala din spatele acestei monede.

3.5 Lucrare practica

3.5.1 Informatii generale

3.5.2 Aspecte importante

3.5.3 Cum subliniaza lucrarea ideea de criptare autentificata

3.6 Bibliografie