

Criptare autentificata si criptomenede

Bejan Octavian Alexandru

April 2018

Facultatea de Informatica,
Universitatea Alexandru Ioan Cuza Iasi

Mic cuprins

1	Introduction	3
2	Tehnologii utilizate	3
3	Mic cuprins	3
3.1	Criptare autentificata	3
3.1.1	Criptarea autentificata	3
3.1.2	Notatii si sintaxa	3
3.1.3	Scheme de criptare	3
3.1.4	Modul de operare	3
3.2	Noi aplicatii ale criptarii autentificate - Ciptomonedele	4
3.2.1	Introducere	4
3.2.2	Utilizare	4
3.2.3	Confidentialitate	4
3.2.4	Integritatea	4
3.2.5	Schema de criptare si autentificare	4
3.2.6	Modul de operare	4
3.3	Aplicatii cunoscute la ora actuala	4
3.3.1	Bitcoin	4
3.3.2	Ethereum	4
3.4	Lucrare practica	5
3.4.1	Informatii generale	5
3.4.2	Aspecte importante	5
3.4.3	Cum subliniaza lucrarea ideea de criptare autentificata . .	5
3.5	Bibliografie	5

1 Introduction

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 utiliza python 3.x deoarece sunt familiarizat cu acesta. In plus se gasesc destule tutoriale despre modul in care poti "programa" criptomonelele (atat bitcoins cat si ethereum).

In limita timpului 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 Criptare autentificata

3.1.1 Criptarea autentificata

Definitie

Cand si de ce este folosita?

3.1.2 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.

3.1.3 Scheme de criptare

Encrypt-then-MAC (EtM)

Encrypt-and-MAC (E&M)

MAC-then-Encrypt (MtE)

3.1.4 Modul de operare

3.2 Noi aplicatii ale criptarii autentificate - Criptomonedele

3.2.1 Introducere

De unde provine termenul, si ce reprezinta.

3.2.2 Utilizare

Cand este folosita.

De cine este folosita.

De ce este folosita.

3.2.3 Confidentialitate

Ce reprezinta confidentialitatea?

Cum ofera criptomonedele confidentialitate?

3.2.4 Integritatea

Ce reprezinta integritatea?

Cum ofera criptomonedele confidentialitate?

3.2.5 Schema de criptare si autentificare

Explicatii pentru fiecare componenta.

3.2.6 Modul de operare

3.3 Aplicatii cunoscute la ora actuala

3.3.1 Bitcoin

Scurt istoric.

Ideea generala din spatele acestei monede.

3.3.2 Ethereum

Scurt istoric.

Ideea generala din spatele acestei monede.

3.4 Lucrare practica

3.4.1 Informatii generale

3.4.2 Aspecte importante

3.4.3 Cum subliniaza lucrarea ideea de criptare autentificata

3.5 Bibliografie