Grigore Eugen-Andrei  
Grupa 202

**Securitate informațională bazată pe metode asimetrice de criptare**

**Cuprins**

**1. Introducere**

Securitatea informațională este o parte importantă a comunicării prin rețelele publice. Există mai multe metode criptografice care asigură securitatea, iar acestea pot fi categorizate în două grupe, simetrice și asimetrice. Metodele simetrice utilizează o singură cheie care poate cripta și decripta mesajul, sau cheia folosită pentru decriptare care este ușor de calculat din cheia de criptare. Metodele simetrice au ca și provocare metoda de împărtășire a cheii intre interlocutori, deoarece este necesar un canal sigur pentru transmisia cheii. Metodele asimetrice rezolvă această problemă prin utilizarea unei perechi de chei, una privată si una publică. Toate mesajele transmise cu cheia publică, pot fi decriptate doar cu cheia privată, iar mesajele criptate cu cheia privată pot fi confirmate ca și provenind de la interlocutorul așteptat. Mărimile cheilor pentru criptare asimetrică sunt de asemenea mai mari decât cele utilizate in criptarea simetrică, ceea ce face compromiterea lor puțin probabilă.

În această lucrare voi discuta despre diferitele metode de criptare asimetrică, utilizarea lor, modul în care au fost folosite în trecut, cum sunt folosite acum, o descriere a sistemelor care utilizează acest tip de criptare, performanța lor și compromisuri pe care acestea le fac. Trebuie sa se țină cont de asemenea că această metodă are și ea neajunsuri. Din acest motiv, lucrarea va mai discuta în scurt și despre alte metode care sunt folosite împreună cu acestea pentru a crea o comunicare cât mai aproape de total sigură.

Într-o lume perfectă, comunicarea poate rămâne sigură cu oricare din metode, cât timp cheile rămân secrete. În acest caz, cheile trebuie știute in prealabil, sau trebuie interschimbate într-un mediu „sanitar”, preferabil fiind ca nimeni să nu știe de existența lor cu excepția interlocutorilor, acest lucru fiind improbabil. Acesta este unul din lucrurile pe care metoda de criptare asimetrică îl rezolvă: asigurarea acestui mediu „sanitar” între doi interlocutori, fie că este utilizat pentru a asigura o altă metodă de criptare, fie că este utilizat ca atare.

**2. Descrierea temei**

**3. Metode asimetrice de criptare**

**4. Concluzie**

**5. Bibliografie**

Apache. (2018). *Apache HTTP Server Version 2.2*. Retrieved from Apache.org: https://httpd.apache.org/docs/2.2/ssl/ssl\_intro.html#cryptographictech

Innokentievich, T. P., & Vasilevich, M. V. (2017). *The Evaluation of the cryptographic strength of asymmetric encryption algorithms.*

Jonathan Katz, Y. L. (2007). *Introduction to modern cryptography.*

K, J., & Lindell, Y. (2022). *2030.*

Menezes, A. J. (1965). *Handbook of applied cryptography .*

Shahzadi Farah, A. S. (2012). *An experimental study on Performance Evaluation of Asymmetric.*

Simmons, G. J. (1979). *Symmetric and Asymmetric Encryption.*