Universitatea Tehnică a Moldovei

CERCETAREA PARTICULARITĂȚILOR METODELOR SIMETRICE DE CRIPTOGRAFIE APLICATE ÎN TELECOMUNICAȚII

Student: **Durbala Anastasia**

Coordonator: **Cerbu Olga**
Conf. univ., dr.

Chișinău, 2021

ADNOTARE

Cercetarea securității informației în aplicarea criptosistemelor bazate pe ecuații eliptice

Cuvinte-cheie: criptosistem, Sistemul Diffie- Hellman, Sistemul ElGamal, Sistemul de criptare Menezes-Vanston.

În această lucrare s-a cercetat metodele, specificul și criptosistemele care au la bază curba eliptică.

Scopul lucrării: Scopul de bază a acestei lucrări este de a cerceta care criptosisteme sunt mai eficiente și care au un timp de procesare cât mai mic, de a deduce care dintre cele trei sisteme de criptare ElGamal, Diffie- Hellman sau Menezes-Vanston au o securitate sporită și poate fi aplicată în domeniile ce necesită o securitate sporită.

Obiectivele: Analiza criptosistemelor Diffie- Hellman, ElGamal și Menezes-Vanston, determinarea prin exemple a metodei și criptosistemului de criptare care poate face față la necesitățile cumpărătorului și este sigură pentru utilizarea pe larg în securitate.

Structura tezei: Lucrarea conține anexe, bibliografie din 13 titluri, iar volumul total al tezei constituie pagini.

În primul capitol se reprezistă informații generale precum definiții, succint este indicat un scurt istoric despre criptare, schema care stă la baza criptării cu curbe eliptice, atacurile care sunt posibile asupra acestui tip de criptare.

În al doilea capitol sunt detaliat explicate criptosistemele care s-au ales pentru cercetare, e dat exemplu de criptare cu fiecare, pentru a înțelege metodologia de securitate a informației.

În capitolul trei se realizează partea economică a acestui proiec și de asemenea se evidențiază care este criptosistemul cel mai de top a secolului XXI.

În urma efectuării calculelor la capitolul economic se ajunge la concluzia care dintre criptosisteme mazate pe curbe elibtice sunt mai eficiente, mai rapide și sigure.

ANNOTATION

Information security research when using cryptosystems based on elliptical equations.

Keywords: cryptosystem, Diffie-Hellman system, ElGamal system, Menezes-Vanston encryption system.

This paper investigates the methods, specifics and cryptosystems that are based on the elliptic curve.

Purpose of the proiect: The main purpose of this paper is to investigate which cryptosystems are more efficient and have the shortest possible processing time, to deduce which of the three encryption systems ElGamal, Diffie-Hellman or Menezes-Vanston have increased security and can be applied in areas that require increased security.

Objectivies: Analysis of Diffie-Hellman, ElGamal and Menezes-Vanston cryptocurrencies, determination by example of the encryption method and cryptosystem that can meet the needs of the buyer and is safe for widespread use in security.

Thesis structure: The paper contains annexes, a bibliography of 13 titles, and the total volume of the thesis is pages.

The first chapter provides general information such as definitions, a brief history of encryption is briefly indicated, the scheme underlying elliptic curve encryption, and possible attacks on this type of encryption.

The second chapter explains in detail the cryptosystems that were chosen for the research, an example of encryption is given with each one, in order to understand the information security methodology.

Chapter three covers the economic side of this project and also highlights the top cryptosystem of the 21st century.

Following the economic calculations, it is concluded which of the cryptosystems based on elliptic curves are more efficient, faster and more secure.

CUPRINS

INTRODUCERE

Criptografia reprezintă o ramură a matematicii care se ocupă cu securizarea informației precum și cu autentificarea și restricționarea accesului într-un sistem informatic. În realizarea acestora se utilizează atât metode matematice (profitând, de exemplu, de dificultatea factorizării nu- merelor foarte mari), cât și metode de criptare cuantică. Termenul criptografie este compus din cuvintele de origine greacă κρυπτός kryptós (ascuns) și γράφειν gráfein (a scrie).

Criptologia este considerată ca fiind cu adevărat o știință de foarte puțin timp. Aceasta cuprinde atât criptografia - scrierea secretizată - cât și criptanaliza. De asemenea, criptologia re- prezintă nu numai o artă veche, ci și o știința nouă: veche pentru că Iulius Cezar a utilizat-o deja, dar nouă pentru că a devenit o temă de cercetare academico-științifică abia începând cu anii 1970. Această disciplină este legată de multe altele, de exemplu de teoria numerelor, algebră, teoria com- plexității, informatică.

Până în vremurile moderne, termenul criptografie se referea aproape exclusiv la criptare, procesul de conversie a informației obișnuite (text în clar) într-un text neinteligibil (text cifrat).[1] Decriptarea este inversul, trecerea de la textul cifrat, neinteligibil, în text clar. Un cifru este o pereche de algoritmi care efectuează atât această criptare cât și decriptarea. Modul de operare de- taliat al unui cifru este controlat de algoritm și de o cheie. Această cheie este un parametru secret (în mod ideal, cunoscut doar celor care comunică) pentru contextul unui anume schimb de mesaje. Cheile sunt importante, iar cifrurile fără chei variabile sunt simplu de spart și deci mai puțin utile. De-a lungul istoriei, cifrurile erau adesea folosite direct pentru criptare și decriptare, fără proceduri adiționale, cum ar fi autentificarea sau testele de integritate.

Eu in această lucrare o să mă axez pe criptarea cu ecuaţii eliptice, şi îmi propun ca obiective:

Să analizez la general cum se criptează cu ecuaţii eliptice;

Să observ metodele de lucru;

Să explic câteva exemple;

Să deduc concluzii pe baza criptării cu ecuații eliptice..

Bibliografie

1. Menezes, A., Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1998.

2. Koblitz, N., *A Course in Number Theory and Cryptography*, ed. a II-a, Springer-Verlag, Ber- lin, 1994.

3. Stinson, D.R., *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

4. Галатенко В.А. *Основы информационной безопасности*: курс лекций – М.: ИНТУИТ.ру, 2006. – 208 с.

5.Чмора А.Л., *Современная прикладная криптология*.-М.:Гелиос АРВ,2001.

6. А.Ю. Зубов.,*Криптографические методы защиты информации. Совершенные шифры*: Учебное пособие. – М.: Гелиос АРВ, 2005. – 192 с.

7. Kaufman C., ed., *The Internet Key Exchange (IKEv2) Protocol*. RFC 4306, Dec 2005. 8.David Kahn, *The Codebreakers*, 1967

*9.*Oded Goldreich. *Stealing Secrets, Telling LiesȘ How Spies and Codebreakers Helped Shape the Twentieth Century, Washington , D.C., Brassey's, 2001*

10. *Curbe eliptice. Aplicații în criptografie*, ©2021. Disponibil: http://docplayer.ro

11. Majalah Ilmiah *Matematika dan Statistika* Volume 15 Nomor 2 2015, 69 – 74 p.

12. *Journal of Theoretical and Applied Information Tehnology*, pag 295, 297

13. *Eliptic-curve Diffie-Hellman*, © 2021. Disponibil: http://www.wikipedia.org/