Universitatea Tehnică a Moldovei

OPERAȚII ÎN CRIPTOGRAFIA APLICATĂ

Masterand: **Zveaghințev Dumitru**

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

Chișinău, 2023

ADNOTARE

Autor: Dumitru Zveaghinţev

Tema: Operații în criptografia aplicată

Cuvintele-cheie: criptografie, informații, securitate, operații din aritmetica modulo.

Structura tezei: Lucrarea conține 3 capitole, bibliografie din 8 de titluri, iar volumul total al tezei constituie 61 de pagini;

Scopul lucrării: Iimplementarea operațiilor din criptografia aplicată utilizate pentru eficacitatea securizării informației.

Obiectivele:

1. Definirea conceptului de curbă eliptică și operațiile de adunare și înmulțire cu o constantă a elementelor sale;
2. Explicația despre modul de efectuare a operației de logaritmare discreta pe o curbă eliptică;
3. Efectuarea criptării si decriptării cu sistemul de criptare Egalam bazat pe operațiile asupra punctelor de pe curba eliptică.
4. Utilizarea operațiilor de exponențiere modulară. Calculul inversei unui număr mare prim modulo.
5. Efectuarea operațiilor de adunare și înmulțire în câmpul Galois. Operații utilizate pentru efectuarea hash-ării criptografice.

Rezultatele obținute: În Teza de master sunt prezentate informații generale despre noțiunea de criptografie și conceptele ei de bază; în același timp sunt prezentate criteriile de clasificare a modelelor de criptare în securitatea informațională; sunt prezentate sisteme de criptare cu chei publice construite pe curbe eliptice; sunt date exemple de operații aplicate în diferite sisteme de criptare.

ANNOTATION

Author: Dumitru Zveaghinţev gr. MMRT-211M

Title: "Operations in Applied Cryptography"

Keywords: cryptography, information, security, *modulo* arithmetic operations.

Structure of the thesis: The work contains 3 chapters, a bibliography of 8 titles, and the total volume of the thesis is 61 pages;

Thesis purpose: The general purpose of the paper is to implement the applied encryption operations used for the effectiveness of information security.

Objectives:

1. Defining the concept of the elliptic curve and the operations of addition and multiplication with a constant of its elements;
2. Explanation of how to perform the discrete logarithm operation on an elliptic curve;
3. Performing encryption and decryption with the Elgamal encryption system based on operations on points on the elliptic curve.
4. Using modular exponentiation operations. Calculating the inverse of a large prime number modulo.
5. Performing addition and multiplication operations in the Galois field. Operations used to perform cryptographic hashing.

The obtained results:

The thesis presents general information about the notion of cryptography and its basic concepts; at the same time, the criteria for classifying encryption models in information security are presented; public key encryption systems built on elliptic curves are presented; more examples of operations applied in different encryption systems are given.

CUPRINS

INTRODUCERE

Dezvoltarea calculatoarelor și a sistemelor de comunicație a sporit necesitatea protejării datelor în formă electronică și a dezvoltării serviciilor pentru asigurarea securității. Un imbold pentru dezvoltarea criptografiei este pozitiv influentat de aparitia lucrarii lui H. Feistel de la IBM, dedicată unei construcții criptografice pentru cifrurile iterative (numite cifruri Feistel), iar în baza acestei construcții, a fost elaborat sistemul de criptare DES și adoptat ca standard de criptare. Acesta a fost considerat standard internațional de criptare cu cheie secreta. Criptografia modernă formează o direcție științifică separată în domeniul matematicii și a informaticii. A devenit o normă aplicarea algoritmilor criptografici în diverse domenii ale activității umane, precum comerțul electronic, transmiterea documentelor semnate electronic, telecomunicații ș.a. Tehnologiile moderne au creat noi oportunități de dezvoltare a criptografiei. Utilizarea Internetului a sporit și mai mult necesitatea asigurării securității informației. Unele aspecte din domeniul securității informației, cum ar fi asigurarea confidențialității, a integrității, autentificării și non-repudierii datelor, reprezintă obiective de bază în criptografia modernă.

Scopul lucrării include bazele necesare înțelegerii principalelor operațiuni utilizate în criptografia aplicată, precum și concepte de securitate a informațiilor și metode criptografice care asigură unele servicii de securitate, precum confidențialitatea, integritatea și nonrepudiarea datelor, autentificarea su

Obiectivele:

1. Definirea conceptului de curbă eliptică și operațiile de adunare și înmulțire cu o constantă a elementelor sale;
2. Explicația despre modul de efectuare a operației de logaritmare discretă pe o curbă eliptică;
3. Efectuarea criptării si decriptării cu sistemul de criptare Elgamal bazat pe operațiile asupra punctelor de pe curba eliptică.
4. Utilizarea operațiilor de exponențiere modulară. Calculul inversei unui număr mare prim modulo.
5. Efectuarea operațiilor de adunare și înmulțire în câmpul Galois. Operații utilizate pentru efectuarea hash-ării criptografice.

Algoritmii criptografici se bazează pe o serie de concepte matematice. Prin urmare, pentru a înțelege criptografia, trebuie mai întâi să stăpânim aceste concepte. Pe parcursul lucrării, elementele teoretice sunt completate cu numeroase exemple, astfel încât cititorul să primească suficiente informații despre aplicarea algoritmilor descriși în rezolvarea problemelor practice.

Principalele rezultate ale prezentării sunt concretizate sub forma unor algoritmi descriși în pseudocod, aproape de implementarea directă într-un limbaj de programare de nivel înalt.

Bibliografia cuprinde lucrări recente, utilizate pe scară largă, care oferă o privire de ansamblu asupra întregului domeniu, precum și aspecte individuale ale problemelor studiate.

CONCLUZII

În această lucrare s-au îndeplinit cu succes toate obiectivele expuse spre realizare și scopul lucrării a fost finalizat cu implementarea în limbajul java a operațiilor descrise în capitolul 3 al lucrării, deasemenea pentru fiecare operație din acest capitol au fost elaborate exemple numerice pentru expunerea operațiilor prin prizma calculelor efectuate în aritmetica modulară. Un loc deosebit în realizarea obiectivelor îl are utilizarea curbelor eliptice în criptarea si decriptarea informației utilizând operații asupra punctelor de pe curba eliptică plană.

1. În matematică, o *curbă eliptică* este o curbă algebrică proiectivă diferențiabilă de genul unu pe care se află un punct dat O. *Ecuația* care satisface o curbă eliptică poate fi considerată peste câmpuri arbitrare și, în special, peste câmpuri finite de interes deosebit pentru *criptografie*. În criptografie, curbele eliptice sunt considerate pe două tipuri de câmpuri finite: câmpuri simple cu caracteristici impare (Z_p, unde p>3 este număr prim) și câmpuri cu caracteristica 2 ($GF(2^m)$).
2. Problema *logaritmului discret* este considerată nerezolvabilă din punct de vedere computațional. Adică, un algoritm clasic eficient pentru calcularea logaritmilor discreti nu este cunoscut deloc. Câțiva algoritmi importanți de criptare cu cheie publică își bazează securitatea pe presupunerea că problema logaritmului discret în grupuri atent selectate nu are o soluție eficientă. Opțiunile populare pentru grupul G în criptografia cu logaritm discret (DLC) sunt grupuri ciclice (Zp) × (cifrul ElGamal; schimbul de chei Diffie-Hellman și algoritmul de semnătură digitală) și subgrupurile ciclice de curbe eliptice pe corpuri finite.
3. Bazat pe problema complexă a calculării logaritmilor discreti într-un câmp finit, *algoritmul ElGamal* ne permite să generăm rapid chei fără a sacrifica securitatea. Folosit în algoritmul de semnătură digitală al standardului DSA DSS.
4. Funcții logaritmice și exponențiale sunt izomorfisme de grup. Deci funcția exponențială crește mai repede decât funcția polinomială, care crește mai repede decât funcția logaritmică. În criptografie, una dintre cele mai importante probleme este că pornind de la funcție reversibilă f – găsim o formă pentru f^{-1}. Inversul unui număr în corpul Zn se poate calcula pe baza Algoritmului lui Euclid extins.
5. Operațiile în câmpul Galois prezentate în subcapitolul 3.2 se utilizează în criptografia aplicată pentru eficacitatea sistemelor simetrice bazate pe blocuri.

BIBLIOGRAFIE

1. D. Stinson and M. Paterson, *Cryptography: Theory and Practice*, 4th ed., Boca Raton, FL: CRC Press, 2019.
2. B. Forouzan*, Criptography&Network Security*, McGraw-Hill Science/Engineering/Math, 2007.
3. W. Diffie and M. Hellman, "*New Directions in Cryptography*," IEEE Transactions on Information Theory, vol. 22, no. 6, p. 644–654, November 1976.
4. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. Chișinău, Editura „Tehnica-UTM”, 2022.
5. С. Сингх, Книга шифров: *Тайная история шифров и их расшифровки*, М.: Астрель, 2009.
6. D. Salomon, *Data privacy and security*, Springer, 2003.
7. H. Gaines, *Cryptanalysis: a study of ciphers and their solution*, Dover Publications, 1939.
8. V. Miller, "*Uses of Elliptic Curves in Cryptography*," in Advances in Cryptology — CRYPTO
9. D. Hankerson, A. Menezes and S. Vanstone*, Guide to elliptic curve cryptography*, Springer-Verlag, 2004.