Ministerul Educației, Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere

Şef departament TSE:

Sava L., conf. univ., dr.

_____

„____”_____ 2020

Analiza și compararea sistemelor de criptare simetrice utilizate in rețele de comunicații

Teză de master

Student: **Bejenari Ion SISRC-191**

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

Chişinău, 2020

REZUMAT

Bejenari Ion

Tema: Analiza și compararea sistemelor de criptare simetrice utilizate in rețele de comunicații

Structura lucrării:

Introducere;

Capitolul 1Descrierea și studierea sistemelor de criptare utilizate in rețele de comunicații;

Capitolul 2 Criptoanaliza lineara;

Capitolul 3 Realizarea algoritmului rc5 și a versiunilor modificate;

Concluzie;

Bibliografia;

Anexe.

Cuvintele-Cheie: Criptare, securitate, criptoanaliza.

Scopul lucrării: Analiza și compararea sistemelor de criptare simetrice utilizate in rețele de comunicații

Obiectivele:

1. Descrierea și analiza sistemelor de criptare utilizate în rețele de comunicații;
2. Efectuarea criptoanalizei lineare asupra sistemului de criptare RC5;
3. Realizarea algoritmilor de criptare RivestCode în mod practic.
4. Elaborarea unei aplicații care va demonstra criptarea și decriptarea algoritmilor din familia RivestCode.

Metodele aplicate: Realizarea numerica a algortmilor si implimentarea în limbalul Java

Rezultatele obținute:

1. Au fost analizată cripto rezistența algoritmilor și punctele sale slabe.
2. A fost realizată criptoanaliza linearaasupra sistemului de criptare RC5
3. Au fost realizate exemple numerice pentru comparare și validare a operațiilor utilizate în metodele de criptare dschise în lucrare.
4. A fost elaborata o aplicație cu interfața grafică. Aplicația permite alegera algoritmului pentru care se ralizează operațiile de criptare și decriptare, respectiv pentru cheia recom

SUMMARY

Bejenari Ion

Theme: Analysis and comparison of symmetric encryption systems used in communication networks

Structure of the paper:

Introduction;

Chapter 1Description and study of encryption systems used in communication networks;

Chapter 2 Linear Cryptanalysis;

Chapter 3 Realization of the rc5 algorithm and modified versions;

Conclusion;

Bibliography;

Anexa.

Keywords: Encryption, security, cryptanalysis.

Aim of the paper: Analysis and comparison of symmetric encryption systems used in communication networks

Objectives:

1. Description of the encryption systems used in communication networks;
2. Performing linear cryptanalysis on the RC5 encryption system;
3. Implementing RivestCode encryption algorithms in a practical way.
4. Development of an application that will demonstrate the encryption and decryption of algorithms in the RivestCode family.

Applied methods: Numerical realization of algorithms and implementation in Java language

The results obtained:

1. The crypto resistance of the algorithms and its weaknesses were analyzed.
2. Linear cryptanalysis was performed on the RC5 encryption system
3. Numerical examples have been made for comparing and validating the operations used in the encryption methods opened in the paper.
4. An application with a graphical interface has been developed. The application allows the choice of the algorithm for which the encryption and decryption operations are performed, respectively for the recommended key.

CUPRINS

INTRODUCERE

Securitatea informațiilor în calculatoare și în sistemele de comunicații este unul dintre cele mai actuale subiecte de astăzi. Astazi majoritatea instituțiilor conectate la rețea suportă pierderi economice din cauza prejudiciilor aduse de defecțiuni ale sistemelor informatice, pătrunderea neautorizată a intrușilor în rețelele lor corporative.

Odată cu trecerea la utilizarea mijloacelor tehnice de comunicare, informața este expusă proceselor aleatorii: defecțiuni și eșecuri ale echipamentelor, erori ale operatorului etc., care pot duce la distrugerea, schimbarea ei în una falsă, precum și crearea premiselor pentru acces persoanelor neautorizate. Cu dezvoltarea continuă și distribuție pe scară largă a tehnologiilor de comunicare a sporit riscul de acces neautorizat la informații (NSD)[1].

Odată cu apariția ACS complexe asociate cu intrarea automată, procesarea, acumularea, stocarea, ieșirea informațiilor, problema de a securiza informația devine și mai importantă. Acest lucru a fost facilitat de:

1 creșterea volumului de informații acumulate, stocate și prelucrate de calculatoare;

2 concentrarea în baze de date comune de informații de diverse programe si accesorii;

3 extinderea cercului de utilizatori cu acces la resurse la un sistem de calcul și matricele de date situate în acesta;

4 complicația modurilor de funcționare a mijloacelor tehnice sistemelor de calcul: introducerea pe scară largă a modului multi-program, partajarea timpului și timpul real;

5 automatizarea schimbului de informații de la mașină la mașină, inclusive pe distanțe mari;

6 o creștere a numărului de mijloace tehnice și de comunicații în sisteme automate de control și prelucrare a datelor.

Sarcina reală de astăzi este organizarea protecției informații în rețelele corporative. Principalele trăsături distinctive rețeaua corporativă poate fi considerată ca administrarea centralizată a rețelei de comunicații și un anumit nivel de conservare și cifrare a informațiilor acumulate și prelucrate în rețeaua corporației, precum și contabilizarea mijloacelor și canalelor de comunicare a tuturor subrețelelor existente.

Cerințele funcționale determină conceptul de securitate a rețelei. Ele determină nu numai configurația rețelei de comunicație, ci și restricții privind utilizarea protocoalelor de rețea. În rețeaua locală (LAN) trebuie separată fizic (conexiune la diverse resurse conectate) servere și locurile de lucru, adică este necesară organizarea locurilor de lucru și a subrețelor de servere. Pentru eficiență funcționarea rețelei ar trebui să fie implementat serviciul de management administrativ, a cărui listă este determinată de arhitectură gestionarea interacțiunii sistemelor

deschise. Această listă include servicii management: performanță, configurare și nume, acreditări, în caz de eșecuri și eșecuri[2].

Pentru a dezvolta o politică de securitate a informațiilor, este necesar de colectat informația care reflectă structura organizației; lista și caracteristicile funcțiilor îndeplinite de fiecare departament și angajați; o descriere a legăturilor funcționale dintre departamente și locuri de muncă separate; lista obiectelor informaționale, circulă în sistem; lista aplicatelor și a sistemului programe; descrierea topologiei complexului de mijloace tehnice. Primit datele sunt procesate și sistematizate. Obiecte de informare poate fi clasificat: pe teme, pe baze ierarhice, după cantitatea estimată de daune cauzate de pierderea unuia sau a altui tip de informații, prin complexitatea recuperării sale. Pentru a îndeplini sarcina este necesar de implimentat metode eficiente de criptare a informatiei pentru a evita modificare, sau furtul informației ceea ce poate duce la perderi material[3].

Scopul lucrării: Analiza și compararea sistemelor de criptare simetrice utilizate in rețele de comunicații.

Obiectivele:

1. Analiza sistemelor de criptare utilizate în rețele de comunicații;
2.Efectuarea criptoanalizei lineare asupra sistemului de criptare RC5;
3.Realizarea algoritmilor de criptare RivestCode în mod practic.
4.Elaborarea unei aplicații care va demonstra criptarea și decriptarea algoritmilor din familia RivestCode.

BIBLIOGRAFIE

[1] A.Leir,C.Richter, W.Banzahf, "Cryptography with DNA Binary Starnds ,"University of Dortmund, Scool of Computer Science, December, 199.

[2] Alexandrescu C - Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne „SI-2007"

[3] Alexandrescu C, Teodorescu C.-Războiul contemporan , Editura Silvy 1999.

[4] A. Joshi, S. T. King, G. W. Dunlap and P. M. Chen, Detecting Past and Present Intrusions through Vulnerability Specific Predicates, SOSP '05: Proceedings of the Twentieth ACM Symposium on Operating Systems Principles, ACM Press, New York, USA, 2005, pp. 91–104.

[5] A. Salomaa, Criptografie cu chei publice, Ed. Militar˘a, 1996.

[6] A. Menezes, P. Oorschot, S. Vanstome, Handbook of Applied Cryptography.

[7] A. Menezes, P. Oorschot, S. Vanstome, Handbook of Applied Cryptography.

[8] Bibhash Roy, Gautam Rakshit, Ritwik Chakraborty, " Enhanced key Generation Scheme based Cryptography with DNA Logic", International Journal of Information and Communication Technology Research,2011.

[9] Internet World Stats: Web Site Directory. Andrew Roos made in 1995 [citat 27.10.2020]. Disponibil: https://netfuture.ch/1995/09/weak-keys-in-rc4/

[10] B. W. Boehm, Software Risk Management, IEEE Computer Society Press, 2001.

[11] C. Alberts, A. Dorofee, Managing Information Security Risks: The OCTAVE Approach, New York: Addison Wesley, 2003.

[12] Denning E. Dorothy Activism, Hacktivism and Cyberterorism (cap. 8), în vol. Network and Networks.

[13] Dr. ing. Virgil Popescu Tehnologia informaţie în spaţiul de luptă modern, în revista Gândirea Militară Românească, nr. 3/2006, pp. 46-50.

[14] Dictionar de biologie -Teofil Craciun, Leonora Craciun.

[15] E. Burtescu, Securitatea datelor în sistemele informatice economice, teză de doctorat, Facultatea de Cibernetică, Statistică şi Informatică Economică, Bucureşti, 2004.

[16] Edith Beral,Mihai Zapan – Chimia Organică.

[17] G. Held, K. Hundley, Arhitecturi de securitate, Editura Teora, 2003.

[18] http://en.wikipedia.org/wiki. Denning E. D., lucr. Cit., p. 26(este la atacul semantic)

[19] Internet World Stats: Web Site Directory. Differential Cryptanalysis Jiazhe Chen, Meiqin Wang, B. Preneel Published 2012 [citat 17.11.2020]. Disponibil: https://www.semanticscholar.org/paper/Impossible-Differential-Cryptanalysis-of-the-Block-Chen-Wang/5d7fe9d3b937e1920f73f36fea8eecf385ed8377

[20] *Brace Schneier,* Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition *John Wiley & Sons, 1996.*