MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șef departament:
Lilia Sava,conf. univ., dr.

_____
„____” _____2021

Cercetarea particularităților metodelor simetrice de criptografie aplicate în telecomunicații

Teză de master

Student: **Burlanescu Mariana gr. SISRC-201M**

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

Chișinău 2021

ADNOTARE

Autor: Burlanescu Mariana

Tema: Cercetarea particularităților metodelor simetrice de criptografie aplicate în telecomunicații.

Cuvintele-cheie: criptare cu cheie secretă, cifru bloc, algoritmii de criptare DES, AES, generarea cheii, cifruri stream, cifruri sincrone, cifruri asincrone, algoritmii de cripate Seal, A5, RC4.

În cadrul acestei lucrări se analizeaza una din metodele simetrice de criptare, și anume metoda de criptare AES.

Scopul: Cercetarea particularităților metodelor simetrice de criptografie aplicate în telecomunicații.

Obiectivele:

1. Familiarizarea cu metodele simetrice de criptografie.
2. Studiul posibilității aplicării metodelor simetrice de criptografie în telecomunicații.
3. Determinarea avantajelor aplicării metodelor simetrice de criptografie în telecomunicații.
4. Analiza detaliată a particularităților algoritmilor metodelor simetrice de criptografie.
5. Cercetarea teoretică detaliată a metodelor simetrice de criptografie.
6. Analiza teoriei despre operațiile în câmpul Galois.
7. De exemplificat utilizarea operațiilor în câmpul Galois.
8. Exemplificarea algoritmului AES.

Era ştiinţifică a criptografiei a început odată cu publicarea în anul 1949 a articolului lui Claude Elwood Shannon (fondatorul teoriei informaţiei, 30.04.1916 – 24.02.2001) *„Communication Theory of Secrecy Systems”*. Începând cu acest moment criptografia devine ştiinţific ramură aparte a matematicii, iar articolul lui Shannon a pus bazele ştiinţifice ale *sistemelor de criptare cu cheie secretă* (sisteme simetrice de criptare).

Trebuie de menționat că în criptografia modernă, indiferent de tipul sistemului de criptare, secretul cifrului se bazează pe păstrarea secretului cheii, și nu a algoritmului de criptare. Mai mult, orice sistem de criptare poate fi spart, considerându-se „bun” acel sistem, costul resurselor pentru spargerea căruia depășește valoarea informației criptate sau timpul cheltuit pentru spargere este prea mare pentru ca informația obținută să mai fie utilă.

ANNOTATION

Author: Burlanescu Mariana.

Title: Research on the peculiarities of symmetric cryptography methods applied in telecomunications.

Keywords: secret key encryption, block cipher, DES encryption algorithms, key generation, stream digits, synchronous ciphers, asynchronous ciphers, Seal, A5, RCA encryption algorithms.

Thesis purpose: This paper analyzes one of the symmetric encryption methods, namely the AES encryption method.

Objectives:

1. Familiarization with symmetric cryptography methods.
2. Study of the possibility of applying symmetric methods of cryptography in telecommunications.
3. Determining the benefits of applyiong symmetric methods of cryptography in telecommunications.
4. Detailed analysis of the particularities of the algorithms of symmetric cryptography methods.
5. Detailed theoretical research of symmetric cryptography methods..
6. Analysis of the theory about operations in the Galois field.
7. For example, the use of operations in the Galois field.
8. Exemplification of the AES algorithm

The scientific era of cryptography began with the publication in 1949 of Claude Elwood Shannon's article (Founder of Information Theory, 30.04.1916 - 24.02.2001) "Communication Theory of Secrecy Systems". From this point on, cryptography became a separate scientific branch of mathematics, and Shannon's article laid the groundwork for secret-key encryption systems (symmetric encryption systems).

It should be noted that in modern cryptography, regardless of the type of encryption system, the secret of the cipher is based on the secrecy of the key, not the encryption algorithm. Moreover, any encryption system can be broken, considering that system "good", the cost of resources for breaking which exceeds the value of the encrypted information or the time spent for breaking is too high for the information obtained to be useful.

CUPRINS

					UTM 0714
Mod	*Coala*	*N.Document*	*Semnat*	*Data*	
Efectuat		Burlanescu M.			**CERCETAREA PARTICULARITĂȚILOR METODELOR SIMETRICE DE CRIPTOGRAFIE APLICATE ÎN TELECOMUNICAȚII**
Verificat		Cerbu O.			
Consultant					
Contr.norm.					
Aprobat		Sava L.			

Lit.	*Coala*	*Coli*
	9	

UTM – FET
SISRC – 201M

INTRODUCERE

Una dintre caracteristicile societății moderne o reprezintă Informatizarea. Tehnologii informaționale noi sunt permanent implementate în diverse domenii ale activității umane. Prin utilizarea calculatoarelor și a software-ului respectiv sunt dirijate procese complexe din cele mai diverse domenii de activitate. Calculatoarele și rețelele de comunicații stau la baza mulțimilor de sisteme de prelucrare a informației, distribuirea ei către utilizator, realizând astfel tehnologii informaționale moderne.

Fără a depinde de mediul fizic prin care se realizeaza (cablu metalic, fibra optică sau mediu wireless) sau de specificul rețelei de transmisie a informațiilor (de calculatoare, de telefonie fixă sau mobilă, de televiziune prin cablu, de distribuție a energiei electrice), securitatea comunicațiilor reprezintă un aspect esențial al serviciilor oferite, fiind critică în cazul informațiilor cu carcater secret din aplicații financiar-bancare, militare, guvernamentale și nu numai acestea. Cu alte cuvinte odată cu dezvoltarea mecanismelor, metodelor și formelor de automatizare a proceselor de prelucrare a informației crește și dependența societății de gradul de securitate a proceselor de gestionare a informației, realizat prin intermediul diverselor tehnologii informaționale aplicate, de care depinde bunăstarea sau uneori și viața multor oameni.

Conexiunea la Internet reprezintă o facilitate dar creează de cele mai multe ori probleme de securitate pentru rețele de comunicații.

Scopul serviciilor de securitate în domeniul rețelelor de comunicații vizează pe de o parte menținerea acestora în funcție (regula celor cinci de 9 adică 99,999% din durata de funcționare), iar pe de altă parte asigurarea securității aplicațiilor și a informațiilor atocate pe suport sau transmise prin rețea.

Se indentifică mai multe aspecte ale securității unei rețele (securitatea accesului fizic și logic, securitatea serviciilor de rețea, secretizarea informațiilor) case se exprimă prin diverși termeni specific: autentigicare, autorizare, asociere cu un cont de utilizator și audi (AAAA – Authentication, Authorization, Accounting, Auditing), confidențialitate, robustețe.

Politica de securitate este cea care, pe baza analizei de securitate a unei rețele, exprimă cel mai bine principiile care stau la baza adopării unei anumite strategii de securitate, implementată prin diverse măsuri specifice, cu tehnici și protocoale adecvate.

Soluționarea problemelor legate de securitatea informației constituie obiectul de studiu al Criptografiei, care este o ramură a matematicii moderne, ce se ocupă de elaborarea metodelor matematice capabile să asigure confidențialitatea, autentificarea și non-repudierea mesajelor, precum și securitatea datelor vehiculate. Criptografia este un set de standarte și protocoale pentru codificarea datelor și mesajelor, astfel încât acestea să poată fi stocate și transmise mai sigur. Ea stă a baza multor servicii și mecanisme de securitate, folosind metode matematice pentru

transformarea datelor, în intenția de a ascunde conținutul lor sau de a le proteja împotriva modificării. Criptografia ne ajută să avem comunicații mai sigure, chiar atunci când mediul de transmitere (de exemplul, Internetul) nu este de încredere. Ea poate fi utilizată pentru a contribui la asigurarea integrității datelor, precum și la menținerea lor în calitate de date secrete, ne permite să verificăm originea datelor și a mesajelor prin utilizarea semnăturii digitale și a certificatelor.

Unul dintre instrumentele principale ale criptografiei este sistemul de criptare, la baza căruia se află algoritmul de criptare, care la rândul său alte categoriile sale în care se împart în dependență de specific.

În această lucrare va fi cercetate particularitățile algoritmului de criptare cu cheie secretă AES.

BIBLIOGRAFIE

1. ZGUREA, Aureliu. *Criptarea și securitatea informației. Note de curs.* Chișinău 2013. 148p.
2. SCRIPCARU, L, BOGDAN I, NICOLAESCU Ș, GHEORGHE C, NICOLAESCU L, *Securitatea rețelelor de comunicații*, Casa de edictură ”Venus” Iași 2008. 193p.
3. Criptografia simetrică. Ciclu de prelegi. Disponibil: https://www.moodle.usm.md
4. АГРАНОВСКИЙ А.В., Хади Р. А., *Практическая криптография, алгоритмы и их програмирование,* Москва, 2009
5. МАО В., *Современная криптография (теория и практика)*, М. Вильямс, 2005
6. Advanced Encryption Standard ©2021. Disponibil: https://ro.wikipedia.org
7. *Raport on the Development of the Advanced Ecryption Standard (AES)*. ©2021 Disponibil: https://www.ncbi.nlm.nih.gov
8. ГАЛАТЕНКО В.А. *Основы информационной безопасности*: курс лекций – М.: 2006-2008 с
9. ЧМОР А.Л. *Современная прикладная криптограф*. М.: Гелиос АРВ,2002. pag. 256 ISBN 5-85438-046-3
10. БАБАШ А.В., ШАНКИН Г.П. *Криптография* М.: Солон-Прессб 2007. – pag. 512 – SIBN 5-93455-135-3
11. ИВАНОВ М.А. *Криптографические методы защиты информации в компьютерных системах и сетях* М.: Кудриц- Образец, 2001. – pag. 363, ISBN 5-93378-021-9
12. СМАРТ Н. *Криптография*. М.: Техносфера, 2005. pag. 528, ISBN 5-94836-043-1
13. *Криптографияю* ©2021. Disponibil: https://www.science.fandom.com
14. ЯЩЕНКО В.В, ВАРНОВСКИЙ Н.П, НЕСТЕРЕНКО Ю.В, КАБАТЯНСКИЙ Г.А, *Введение в криптографию*. Москва Издательство МЦНМО 2012 ISBN 978-5-4439-0026-1
15. СИНГХ С. *Книга шифров. Тайная история шифров и их расшифровки.* М.: Аст, Астрель, 2006. pag. 447 ISBN 978-5-17-038477-8