



UNIVERSITATEA TEHNICĂ A MOLDOVEI

**Securitatea informației cu sisteme
bazate pe blocuri**

Information security systems based on blocks

Masterand:

Mindrigan Dumitru

Conducător:

Lect. sup Melnic Radu

Chișinău 2016

Ministerul Educa•iei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Catedra Automatică și Tehnologii Informaționale

Admis la sus•inere

Șef de catedră: prof univ, dr. Victor Beșliu

”_____” _____ 2016

SECURITATEA INFORMAȚIEI CU SISTEME BAZATE PE BLOCURI

Teză de master în Tehnologii Informaționale

Masterand: _____ (D.Mindrigan)

Conducător: _____ (R. Melnici)

Chișinău 2016

ADNOTARE

Asupra lucrării de master cu tema “Securitatea informației cu sisteme bazate pe blocuri” elaborată de masterandul Mindrigan Dumitru. Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației de aceea dezvoltarea tehnologică a fost acompaniată și de soluții de securitate cu sisteme bazate pe blocuri.

Structura logică a lucrării constă din 4 capitole de bază, surse bibliografice, concluzii și anexe. În capitolul I, Noțiunile privind securitatea informațiilor se definesc noțiuni de securitate a informațiilor. În capitolul II, se descrie politica de securitate informațională. În capitolul III, sunt reprezentate metode de atac asupra algoritmilor Rivest-Code. În capitolul IV, sunt descriși algoritmi Rivest-Code.

Argumentarea actualității temei constă în analiza și caracterizarea situației curente în domeniul securității informației, concret în compartimentul securității cu sisteme pe blocuri de tipul Rivest Code cât și o analiză comparativă a tuturor versiunilor existente și utilizate în securitate, reieșind din aplicarea rezultatelor preconizate. Rezultatele obținute sunt în bună corelație cu scopurile și conținutul cercetării.

ADDNOTATION

Master's thesis on the topic "Information security systems based on blocks" developed by Master Mindrigan Dumitru. Information security is a broader concept that refers to ensuring the integrity, confidentiality and availability of information that technological development has been accompanied and security solutions based system blocks.

The logical structure of the paper consists of four main chapters, bibliographic sources, conclusions and annexes. In Chapter I, Getting define information security information security concepts. Chapter II describes the Information Security Policy. In Chapter III, are the methods of attack on the algorithms Rivest-Code. In Chapter IV, the algorithms described Rivest-Code. Timeliness argument is to analyze and characterize the theme of the current situation in the field of information security, systems security compartment concrete blocks Rivest Code such as a comparative analysis of all existing versions used in security resulting from the application of the expected results. The results are in good correlation with the aims and content of the research.

Cuprins :

Introducere	6
1. Noțiuni privind securitatea informațiilor	8
1.1. Definiția noțiunii de securitatea Informațiilor	8
1.2. Secțiunile standardului de securitate ISO / IEC 17799.	10
1.2.1. Politica de securitate	10
1.2.2. Organizarea securității.....	10
1.2.3. Clasificarea și controlul activelor	11
1.2.4. Securitatea personalului	11
1.2.5. Securitatea fizică	12
1.2.6. Managementul comunicațiilor și al operării.....	13
1.2.7. Controlul accesului	14
1.2.8. Dezvoltarea și întreținerea sistemului	16
1.2.9. Planificarea continuității afacerii	16
1.2.10. Conformitatea	17
2. Politica de securitate informațională.....	18
2.1. Generalități despre politica de securitate.....	18
2.2. Scopul politicii de Securitate.....	18
2.3. Obiectivele politicii de securitate	19
2.4. Principiile de realizare a politicii de securitate.....	20
2.5. Gestionarea riscurilor	20
2.6. Clasificarea informației.....	21
2.7. Atribuții și responsabilități	22
3. Criptografia și metode de atac asupra algoritmului Rivest – Code	23
3.1. Metode de atac în criptografie asupra algoritmului Rivest-Code	27
3.2. Atac cu text cifrat.....	29
3.3. Atac cu text clar ales.....	29
3.5. Atacul omului de la mijloc	30
3.6. Atac cu întâlnire la mijloc	31
3.8. Atacuri prin interpolare	33
3.9. Atacuri ”divide și cucerește”	34

3.8. Atacuri prin interpolare	33
3.9. Atacuri ”divide și cucerește”	34
4. Descrierea Algorimilor Rivest- Code	35
4.1. Algoritmul RC2.....	35
4.2. Algoritmul RC4.....	37
4.3. Algoritmul RC5.....	38
4.3.1. Extinderea cheii	39
4.3.2. Criptarea RC5.....	40
4.3.3. Decriptarea RC5	41
4.4. Cifrul de criptare pe bloc RC6	42
4.4.1. Descrierea algoritmului	42
4.4.2. Detalii despre RC6.....	42
4.4.3. Planul de chei.....	43
4.4.4 Criptare și decriptare.....	43
4.4.5. Probleme de implementare	45
4.4.6. Design și motivație	45
4.4.7 Securitate și simplitate.....	45
4.5. Securitate.....	46
4.6. Analiza comparativă a algoritmilor	47
4.7. Flexibilitate și Scopuri de viitor.....	50
Concluzii	52
Bibliografie	54