

Universitatea Tehnică a Moldovei

**Studierea tehnicilor si algoritmilor de securizare a
datelor in retea**

**Study of network security techniques and
algorithms**

**Masterand:
Șerban Andrei**

**Conducător:
lect.univ. Bulai Rodica**

Chișinău – 2018

Rezumat

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. Lucrul în rețea și conectarea la Internet induc și ele riscuri suplimentare, de acces neautorizat la date sau chiar fraudă.

În lucrarea dată au fost studiați algoritmi de criptare și decriptare a datelor, precum și tehnicile de creare a programelor pentru criptarea datelor.

Ca rezultat, s-a prezentat o abordare modernă de proiectare a unei aplicații de securizare a fluxului de date în timpul transmiterii informației prin intermediul rețelei de calculatoare. Unul din punctele forte ale acestui sistem este utilizarea algoritmului AES pentru transmisiunea datelor pe server.

Unul din punctele forte ale aplicației este modalitatea de transmisiune a fluxului de date deoarece fluxul este împărțit în mai multe părți și codificat cu cheie de criptare. Odată ajuns la server el este decriptat și apoi transmis utilizatorului final.

Abstract

Information security is a broader concept that refers to ensuring the integrity, confidentiality and availability of information. The dynamics of information technology incite new risks for which organizations need to implement new control measures. Networking and Internet connection also cause additional risks, unauthorized access to data or even fraud.

In this paper, encryption and decryption algorithms were studied, as well as the techniques for creating programs for data encryption.

As a result, a modern approach to designing a data flow securing application during the transmission of information via the computer network was presented. One of the strengths of this system is the use of the AES algorithm for data transmission on the server.

One of the strengths of the application is the way the data stream is transmitted because the stream is divided into several parts and coded with an encryption key. Once it has reached the server it is decrypted and then transmitted to the end user.

Cuprins

Introducere	8
1 Analiza domeniului de cercetare	9
1.1 Sisteme criptografice	9
1.2 Aspecte de bază a securității în rețea	14
1.2.1 Filtrarea adreselor MAC	14
1.2.2 Firewall	15
1.2.3 Protecția transmisiunilor prin criptare	17
1.3 Enunțul problemei	17
2 Algoritmi de criptare a informației	19
2.1 RSA (Rivest Shamir Adleman)	19
2.2 (Pretty Good Privacy)	20
2.3 IDEA (International Data Encryption Algorithm)	23
2.4 Modalități de spargere a codurilor	24
2.4.1 Atacul de forță brută	24
2.4.2 Atacuri mai rapide decât forța brută	25
2.4.3 Spargere a codurilor RSA	26
3 Realizarea aplicației	29
3.1 Platforma .Net Framework	29
3.2 Tehnologia ADO.NET	30
3.3 Limbajul C	31
3.4 Selectarea algoritmului de criptare	34
3.5 Descrierea modulelor sistemului informațional	39
3.6 Descrierea aplicației	42
Concluzie	57
Bibliografie	58