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

Chişinău – 2018

Rezumat

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

În lucrarea dată au fost studiați algortmii de criptare și decriptate 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