Frequency cryptanalysis. Caesar cipher

Mariia Manuylova

Peter the Great St.Petersburg Polytechnic University

masha-loverus@yandex.ru

October 21, 2016

Abstract

I. Introduction

Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques. Cryptology is the study of cryptography and cryptanaylsis. Key features of information security information include confidentiality or privacy, data integrity, authentication, and nonrepudiation. Each of these aspects of message security can addressed by standard methods in cryptography.

Frequency cryptanalysis cryptography is one of the sections. This is one of the simple methods of encryption and decryption of text. It studied the frequency of occurrence of letters in various texts and based on the detected results to the decryption key for a particular text.

Cipher is a map from a space of plaintext to a space of ciphertext. We was studied the Caesar cipher. This is the easiest method based on the frequency cryptanalysis. This article was previously studied by the task of decoding the encoded text with the frequency of cryptanalysis using the Caesar cipher.

II. Methodology

III. Experiment

IV. Result

V. Discussion

VI. Reference