УДК 004.056.55

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ МЕТОДОМ ПОДПИСИ ЛАМПОРТА

Головченко О. Н.

магистрант

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Новочеркасск, Россия

Оганян Р. Г.

аспирант

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Новочеркасск, Россия

Аннотация.

В данной статье осуществлена программная реализация методом криптографической защиты с помощью подписи Лампорта. Описывается алгоритм подписи Лампорта.

Ключевые слова: криптографическая защита, подпись Лампорта, криптостойкость, хеширование.

SOFTWARE IMPLEMENTATION OF CRYPTOGRAPHIC PROTECTION BY THE LAMPORT SIGNATURE METHOD

Golovchenko O.N.

master student

South-Russian State Polytechnic University (NPI)

Novocherkassk, Russia

Oganyan R.G.

graduate student

South-Russian State Polytechnic University (NPI)

Novocherkassk, Russia

Abstract

In this article, implemented software implementation of the method of cryptographic protection using the signature Lamport. The Lamport signature algorithm is described.

Key words: cryptographic protection, Lamport signature, cryptographic strength, hashing.

Signature Lamport is a public-key digital signature cryptosystem. Can be built on any one-way function. It was proposed in 1979 and named after its author, an American scientist, Leslie Lamport. The cryptographic strength of Lamport's signatures is based on the robustness of the hash function. For each hash function that generates n-bit digest, perfect resistance to the restoration of the pre-image and to the restoration of the second pre-image implies for each execution of the hash function 2^n operations and 2^n bits of memory in the classical computational model using Grover's algorithm, restoring the preimage of the ideal hash function is bounded from above $O(2^{n/2})$ operations in a quantum computational model [1].

Signature Lamport as follows:

The sender hashes the message with the n-bit hash function. Creates n pairs of random numbers and hashes them, thereby obtaining the public key. Then, for each bit in the message hash, it takes the corresponding number from the secret key. If, for example, the first bit in the message hash is zero, it takes the first number from the first pair of the secret key. If the first bit is one, it uses the second number in the first pair. These numbers constitute the signature of the sender.

Further the message goes with the attached signature. The recipient accepts the message hash it with an n-bit hash function. Then, for each bit in this hash, he selects a number from the sender's public key. Afterwards, the recipient hashes each of the n numbers from the sender's signature and gets n hashes. If these n hashes exactly match the n hashes that he just received from the sender's public key, the recipient considers the signature to be authentic. If not, then fake.

Software implementation.

When you start the application, the main form appears, as shown in Figure 1.

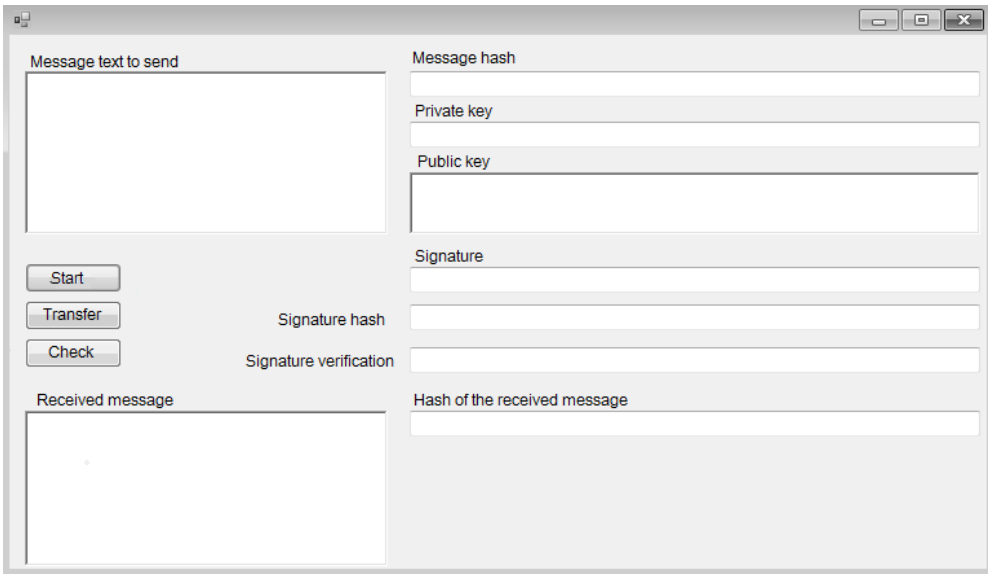

Fig.1 - Main Application Form

Next, the user enters a message for transmission and presses the "Start" button. After that, the program calculates the message hash, generates the private key, hashes the private key, calculates the message signature, its hash, and displays all the information in the appropriate fields on the form. The result is shown in Figure 2.

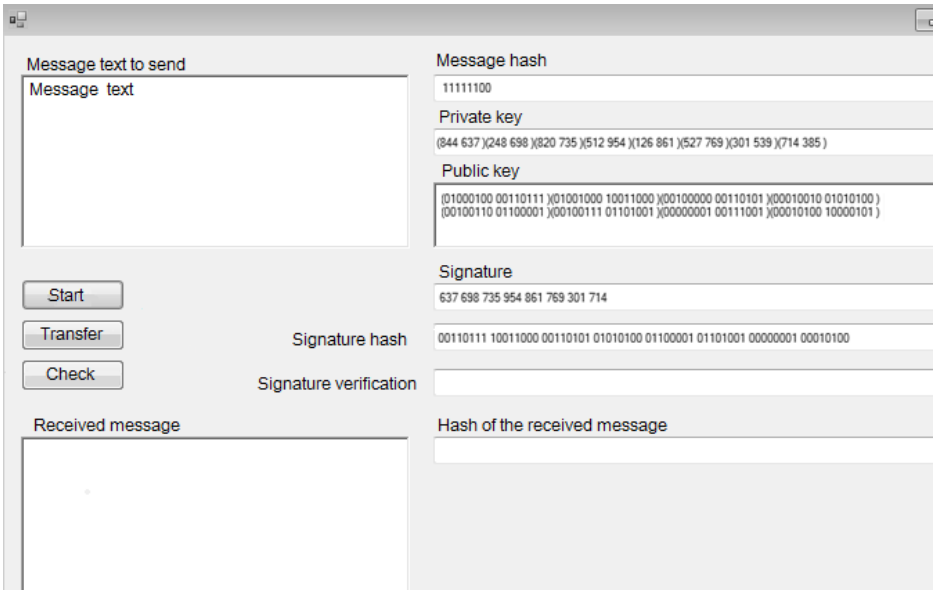

Fig.2 - The result of the start button operation

Next, the user transmits the message by clicking on the "Transfer" button (Figure 3).

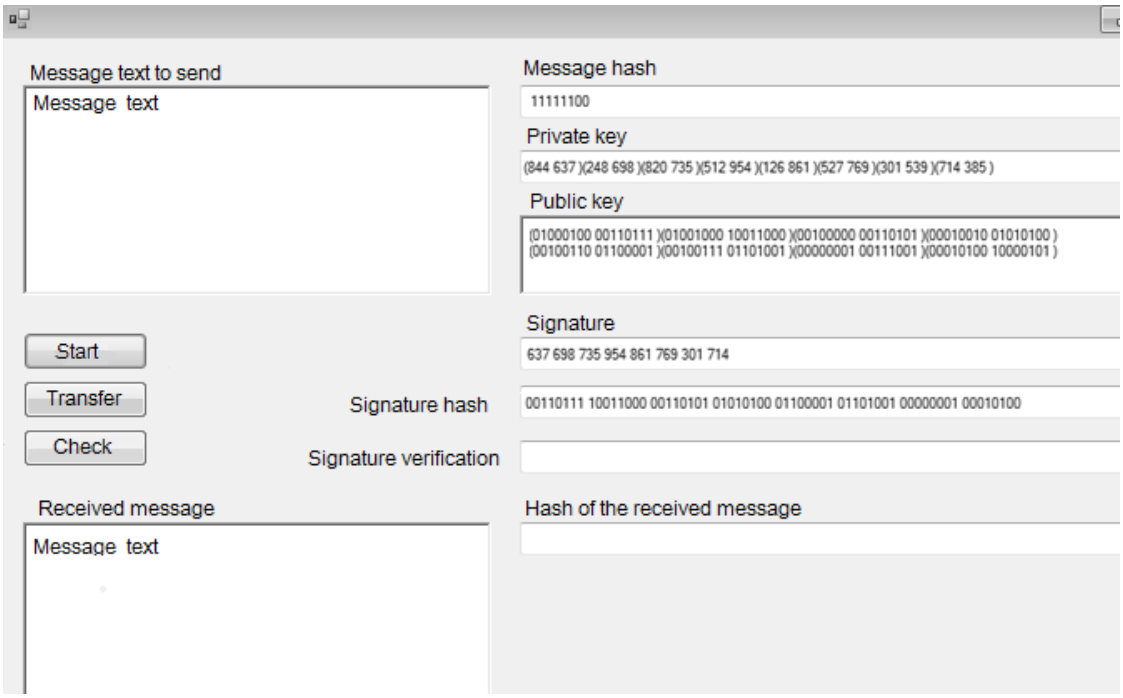

Fig.3 - Message Transfer

Then, the signature of the message is verified by creating a hash of the transmitted message. Further, for each bit of the hash, a number is selected from the public key, and if the resulting sequence matches the signature of the message, the signature is considered genuine. The result of the test is presented in Figure 4.

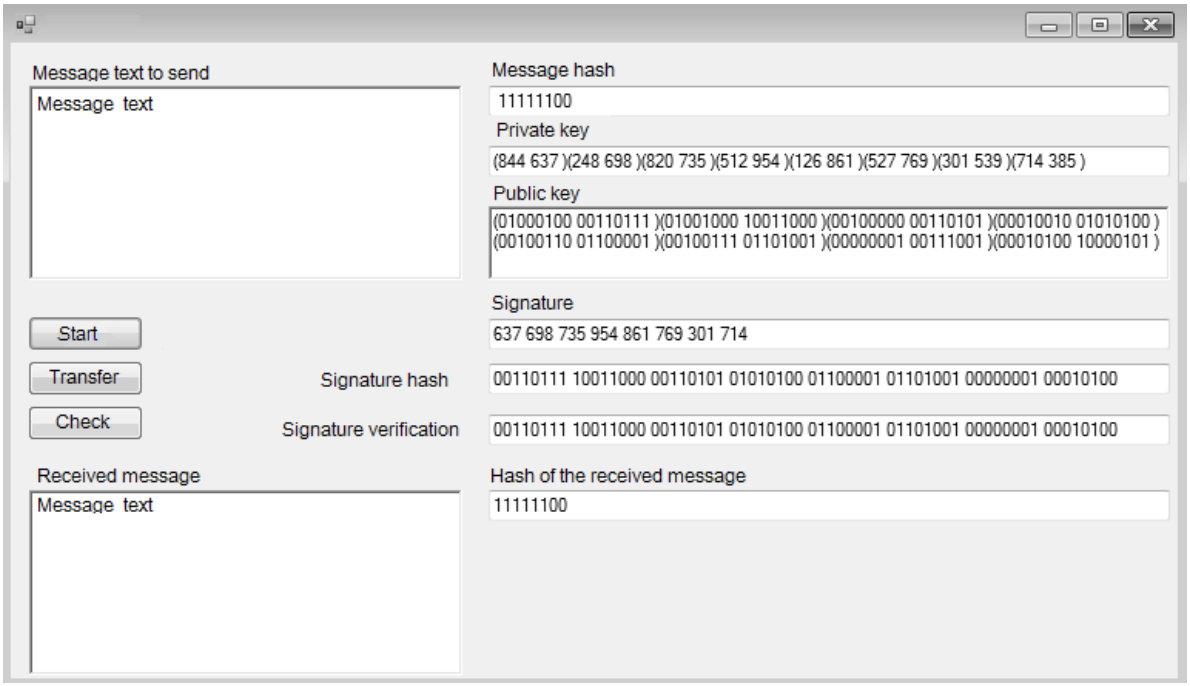

Fig.4 - Signature Verification Result

Thus, this system is easy to use, but it has at least two obvious drawbacks. First, a preliminary transfer of the verification parameters is required. Secondly, and more importantly, the signature greatly increases the length of the message.

References :

1. Signature Lamport [Electronic resource]. - Access mode: https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0% BF% D0% B8% D1% 81% D1% 8C_% D0% 9B% D1 % 8D% D0% BC% D0% BF% D0% BE% D1% 80% D1% 82% D0% B0 (circulation date 12/20/2018).

Оригинальность 96%