ENCRYPTON APPLICATION

Dadenova Gulxan Kenesbaevna
Uzbekistan, Tashkent ,
Tashkent University of Informational Technologies, Assistant

Maxammadjonov Maxammadjon Alisher o'g'li
Uzbekistan, Tashkent ,
Tashkent University of Informational Technologies, student

Abstract. The word encryption comes from the Greek word kryptos, meaning hidden or secret. The use of encryption is nearly as old as the art of communication itself. As early as 1900 BC, an Egyptian scribe used non-standard hieroglyphs to hide the meaning of an inscription. In a time when most people couldn't read, simply writing a message was often enough, but encryption schemes soon developed to convert messages into unreadable groups of figures to protect the message's secrecy while it was carried from one place to another. The contents of a message were reordered (transposition) or replaced (substitution) with other characters, symbols, numbers or pictures in order to conceal its meaning.

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-rand omen cryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

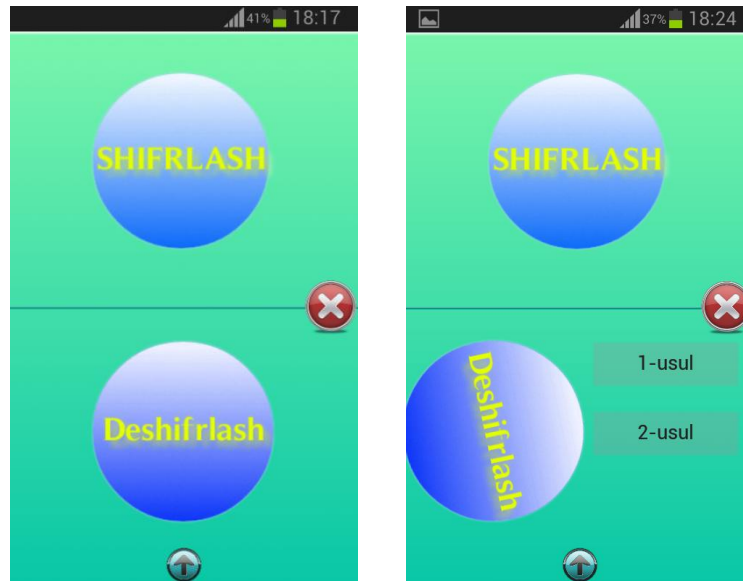*Keywords: encryption, decipherment, message, information security*

This program will run Android and Windows platforms. Each user shiflrashi and text data using the software, it can deshifrlashi. This is more like WhatsApp SMS Telegram correspondence is used to encrypt messages.

This program will ensure the security of the data being sent and received text. The program created in C ++ and compiled for the Android platform and the Windows operating system.
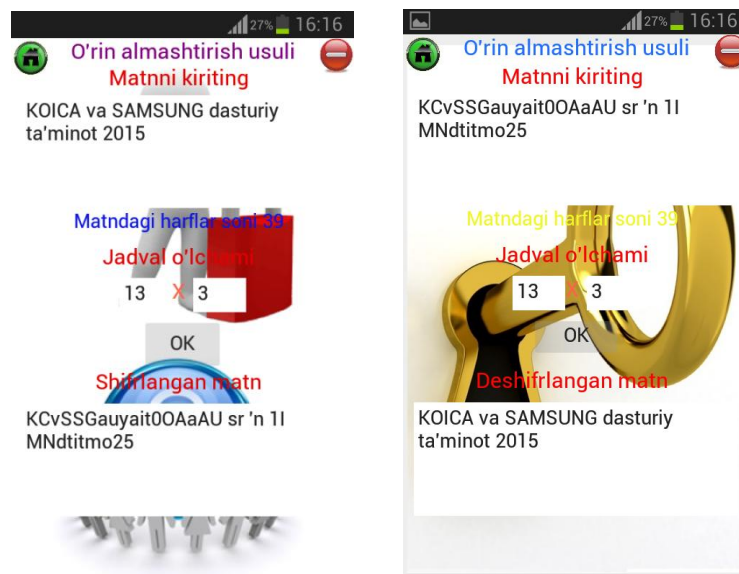
Encryption is meant to make it impossible to read the messages, in other words, is the encoding.

Could become the decipherment of the encrypted text. Each key is used in both cases. Will be discussed in more detail below.

Messages via two methods of encryption and decipherment program.

Method 1 Change the text in the table on the basis of the encryption method, the table serves as the key size. Exchange encrypted text instead of letters. The number of letters to write plays an important role in the size of the table. After typing the text written several letters about the message, depending on the size of the table. For example, if the 24 letters should be included as a 6x4 table the size of a tub the size of the table if more numbers are numbers that you can write. If, for example 37 table size as you can get 8x5 = 40. The rest of the criteria for the program itself '*' sign. The size of the table serves as key. How to send key shifrlasa, the parties need such a key deshifrlashi. Mobile application skrinshotini see in the picture below and you can understand how coriander.

This text encryption and decipherment can see it in the picture.

2-way through a keyword in the text confidential. This is referred to as the method of information security "gamma". After writing the text the key word, the key word should be the size of the text size on the floor. The other does not play a role in the length of the keyword. Any text encryption can be used as a keyword. In decipherment enough to write encrypted key by typing text into the blank. The advantages of this method is that two people knew the keyword, it is also possible to send and receiv. So this method is stronger privacy.
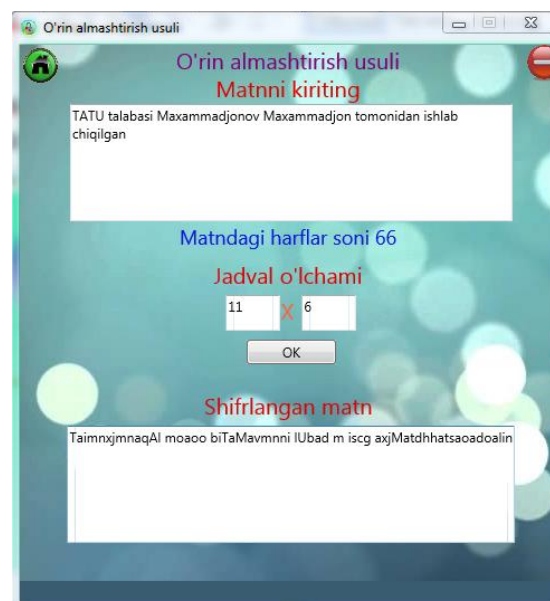
This way you can understand the picture that is displayed:

2-way through the encryption and decipherment. As the key word "Tatu" is used.

Will be available:

Many people in their SMS messages (social networks, messenjerlarda) want to ensure safety. Through this program, you can achieve these desires. Currently, most of the Android phones use this creates a very easy app to use them.

For the Windows operating system is as follows:

Program created by authors Maxammadjonov Maxammadjon and Dadenova Gulxan.

REFERENCES

1. Cracking the Coding Interview, 6th Edition: 189 Programming Questions and Solutions, Gayle Laakmann McDowell 2015

2. CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide, Darri Gibson 2014