

e-Nigma

Purpose:

The e-Nigma is to protect content files (including classified documents from access by third parties). The protection is realized by encrypting the file by 128 bit key of RC4 algorithm, produced from the password entered by the user.

In practical terms for the lack of familiarity with the 128 bit key does not already know the content of an encrypted file.

RC4 algorithm is a widely used symmetric key encryption developed by RSA Data Security Inc.. The algorithm uses a key to encrypt and decrypt the information and requires a relatively small surcharge calculation.

Requirements:

Microsoft Windows 95/98, Windows NT and higher (Windows 2000, XP, Vista).
Internet Explorer 5.5 or higher with 128 bit encryption strength or higher.

Functionality:

The e-Nigma is integrated in Windows Explorer shell and the email program. Setting the mouse cursor to any file and click the right mouse button to display the context menu of the command: Encrypt the file with the extension other than. "enigma" or Decrypt - for files with the extension. "enigma". All software components are installed to instalation folder.

Description:

Użytkownik selects a file to encrypt or deciphering. Enter the password confirmation. The password is haszowane algorithm MD5. Then, the obtained Hashana symmetric key is generated with a length of 128 bits or 40 bits - set by the user. At the end of the content of the file is encrypted kromkami using symmetric key algorithm, RC4.

The resulting file is the same size as the source.

The source file after successful encryption is deleted - see deleting the source file.

To restore the contents of an encrypted file, it is necessary to know the password you used for encryption. Ignorance of the password - prevents the reproduction of the content of the file. Passwords are not stored in the system.

Encryption strength

An important issue for safety length of encrypted information is used keys (eg 128 bits). The keys are longer, the harder it is to decrypt the information. It is widely agreed that:

1. for asymmetric keys: 512 - is too low, 768 - a relatively safe, 1024 - strong safety.
 2. for symmetric keys: 40 - is too little, 56 - relatively safely, 128 - strong safety.
- Violations of the key method of brute force (check the possible keys in sequence).
1. Breaking 40 bit key, took 3 hours the network computers.
 2. Breaking 56 bit key (in the RC5 algorithm) took 250 days in one of the projects distributed.net. The experiment was carried out by a network of computers, whose performance was equivalent to 26 tysięcycom desktop Pentium 200.
 3. Breaking 128 bit key would take 1 trillion x 1 trillion years (using a single supercomputer).

Software updates:

Updates are available from the menu updates,
or location: <http://www.e-msoft.com>

Specifications:

Encryption algorithm: RC4.

Key length: 128 bits.

Delete the original file: once blurring of the public content.

Reducing the length of the file: no restrictions.

Trademarks:

Microsoft, Windows - are registered trademarks of Microsoft Corporation.