What is Shifrovalshik?

Shifrovalshik (Russian: the one who encrypts, cryptoman)

The software program Shifrovalshik is a file-encryption tool that works with U.S.S.R. GOST 28149-89 algorithm. 256bit key, Operation mode: OFB You may use passwords in your own language (Russian, Ukrainian, etc).

GOST 28147-89 is a Soviet and Russian government standard symmetric key block cipher.

If you need Russian version of this program you may download it from our web site.

If you want to encrypt your e-mail you may open Notepad or MS Word type your letter after that save it as a file. Encrypt it, zip it with WinZip (Compressed folder under XP) and attach the file to your message.

Espanol

La herramienta del cifrado funciona con algoritmo del GOST 28149-89 de la URSS. 256bit llave, modo de la operacion: OFB puedes utilizar contrasenas en tu propia lengua (ruso, ucraniano, etc). El GOST 28147-89 es una cifra dominante simetrica estandar del bloque del gobierno sovietico y ruso.

DE

Verschlusselungwerkzeug arbeitet mit Algorithmus DES UdcSsr GOSTS 28149-89. 256bit Schlussel, Betrieb Modus: OFB kannst du Kennworter in deiner eigenen Sprache (russisch, ukrainisch, usw.) verwenden. GOST 28147-89 ist eine sowjetische und russische Regierung symmetrische Schlusselblockstandardziffer.

Russian

Работает по алгоритму ГОСТ (ГОСТ 28147-89), длина ключа 256 бит режим шифрования OFB. 3-я редакция. Криптостойкость повышена на 20 процентов (за счет хеширования), переработаны алгоритмы хешированя заменены на более надежные в 256 бит, увеличена длина вводных ключей до 120 бит, введена система банковского шифрования. Также есть возможность шифрования конфиденциальных данных сроком до 2036 года.

Why is encrypting your E-mail important?

Unless you are an arms dealer, a drug dealer, a child pornographer, or some sort of other crimianal or deviant, you don't have any need for public key encryption, right? Wrong. When you write sombody a letter, and put in an envelope, you don't know for certain that nobody other than you and the person to whom you wrote the letter are reading it. However, you can be pretty sure that every postman and other random individual along the way is not opening the envelope, if it arrives sealed at its destination. Similarly, when you talk on the phone, you don't know that it isn't tapped, but tapping a phone is a non-trivial task that at least requires a little effort on the part of the would-be evesdropper. E-mail is a different matter. E-mail is intrinsically about as secure and private as using smoke signals to send your personal correspondence. I'm not just talking about people looking over your shoulder, or people breaking into your account and reading your private files. The instant you send a message out on the internet, you have broadcast it to the entire world. It is very easy for somebody other than the recepient of an E-mail message to collect the data packets off of the net and intercept your message--without either you or the receipient of the message knowing that the message has been intercepted. If you want an example of how easy it is for somebody to monitor every keystroke you type on a computer without your knowledge, read The Cuckoo's Egg by Cliff Stohl. Just think: do you want any random, or not-so-random, individual to be able to read the private letters you write to your best friend, your mother, or your girlfriend/boyfriend?

You don't really even have a modicum of privacy if you send this sort of E-mail unecrypted. The only way you can be even reasonably sure that nobody other than those you want to are reading the messages is to encrypt them with something like PGP or RIPEM. And this does not even get into things like industrial research or scientific secrets, where E-mail is a very convenient way to communicate, but a lot is at stake if it is not secure. Most "cipherpunks" will laugh or yell at you if you raise the issue of child pornographers and the like using cryptography to dodge law enforcement. The truth is, this is a real problem. However, there are other things in the USA, like freedom of speech, freedom of the press, the right to bear arms, and so forth, which make life easier for criminals, but which most people would not want to give up in the name of law enforcement. It's a tradeoff. My point simply here is that normal, decent people do have a use and a need for encrypting their E-mail, and as such you shouldn't feel like a deviant if you do it, nor should you assume that people who do it are necessarily deviants.

Robert A. Knop Jr. / rknop@panisse.lbl.gov

If you are mailing a check to pay a bill or perhaps a letter telling a friend or family member that the extra key to your house is hidden under the large rock to the left of the back porch you might use a security envelope with hatched lines to obfuscate or hide the contents of the envelope even better. The post office offers a number of other means of tracking messages- sending the letter certified, asking for a return receipt, insuring the contents of a package, etc.

Why then would you send personal or confidential information in an unprotected email? Sending information like the location of your extra house key under the large rock to the left of the back porch in an unencrypted email is the equivalent of writing it on a postcard for all to see.

About GOST

General
Designer(s): USSR
First published: 1990
Cipher detail
Key size(s): 256 bits
Block size(s): 64 bits
Structure: Feistel network
Rounds: 32

Developed in the 1970s, the standard had been marked "Top Secret" and then downgraded to "Secret" in 1990. Shortly after the dissolution of the USSR, it has been declassified and released to the public. GOST 28147 was a Soviet alternative to the United States standard algorithm, DES. Thus, the two are very similar in structure.

GOST has a 64-bit block size and a key length of 256 bits. Its S-boxes can be secret, and they contain about 512 bits of secret information, so the effective key size can be increased to 768 bits; however, a chosen-key attack can recover the contents of the S-Boxes in approximately 232 encryptions (Saarinen, 1998).

GOST is a Feistel network of 32 rounds. Its round function is very simple: add a 32-bit subkey modulo 232, put the result through a layer of S-boxes, and rotate that result left by 11 bits. The result of that is the output of the round function. In the diagram to the left, one line represents 32 bits.

The subkeys are chosen in a pre-specified order. The key schedule is very simple: break the 256-bit key into eight 32-bit subkeys, and each subkey is used four times in the algorithm; the first 24 rounds use the key words in order, the last 8 rounds use them in reverse order.

The S-boxes accept a four-bit input and produce a four-bit output. The S-box substitution in the round function consists of eight 4 ? 4 S-boxes. The S-boxes are implementation-dependent - parties that want to secure their communications using GOST must be using the same S-boxes. For extra security, the S-boxes can be kept secret. In the original standard where GOST was specified, no S-boxes were given, but they were to be supplied somehow. This led to speculation that organizations the government wished to spy on were given weak S-boxes. One GOST chip manufacturer reported that he generated S-boxes himself using a pseudorandom number generator (Schneier, 1996).

http://en.wikipedia.org/wiki/GOST_28147-89

Secure download

- shifroval.zip (Russian edition)
- shifroval_eng.zip (English edition)

E-mail contact:

Denis I. Zabiyako (zabiyakod@mail.ru)