PROCEEDINGS

of the Union of Scientists - Ruse

Book 5

Mathematics, Informatics and Physics

Volume 11, 2014

RUSE

PROCEEDINGS
OF THE UNION OF SCIENTISTS - RUSE

Union of Scientists - Ruse
16, Konstantin Irechek Street
7000 Ruse
BULGARIA
Phone: (++359 82) 828 135,
(++359 82) 841 634
E-mail: suruse@uni-ruse.bg
web: suruse.uni-ruse.bg

Contacts with Editor
Phone: (++359 82) 888 738
E-mail: zzdravkova@uni-ruse.bg

PROCEEDINGS
of the Union of Scientists – Ruse

ISSN 1314-3077

ISSN 1314-3077

Proceedings

of the Union of Scientists– Ruse

Contains five books:

1. Technical Sciences
2. Medicine and Ecology
3. Agrarian and Veterinary Medical Sciences
4. Social Sciences
5. Mathematics, Informatics and Physics

The Ruse Branch of the Union of Scientists in Bulgariawas foundedin 1956. Its first Chairman was Prof. StoyanPetrov. He was followed by Prof. TrifonGeorgiev, Prof. KolyoVasilev, Prof. Georgi Popov, Prof. MityoKanev, Assoc. Prof. Boris Borisov, Prof. Emil Marinov, Prof. HristoBeloev. The individual members number nearly 300 recognized scientists from Ruse, organized in 13 scientific sections. There are several collective members too– organizations and companies from Ruse, known for their success in the field of science and higher education, or their applied research activities. The activities of the Union of Scientists – Ruse are numerous: scientific, educational and other humanitarian events directly related to hot issues in the development of Ruse region, including its infrastructure, environment, history and future development; commitment to the development of the scientific organizations in Ruse, the professional development and growth of the scientists and the protection of their individual rights.

The Union of Scientists – Ruse (US – Ruse) organizes publishing of scientific and popular informative literature, and since 1998 – the "Proceedings of the Union of Scientists- Ruse".

BOOK 5

"MATHEMATICS, INFORMATICS AND PHYSICS"

VOLUME 11

CONTENTS

Mathematics

Informatics

BOOK 5

"MATHEMATICS, INFORMATICS AND PHYSICS"

VOLUME 11

Physics

web: suruse.uni-ruse.bg

DATA ENCRYPTION SOFTWARE

Victoria Rashkova

Angel Kanchev University of Ruse

Abstract: *One of the main problems for all users is the protection of their personal data. This article presents the basic cryptographic algorithms. Different software products for data encryption are presented. A relational database for comparison between them was created using the following parameters: price, size of the key platform use encryption method, users, opportunities, support. The advantages and disadvantages of the chosen software to facilitate user choice are presented.*

Keywords: *encryption, decryption, bit size key, data security, encryption software.*

INTRODUCTION

One of the big problems with the development of information technology becomes the protection of user data. It is important that the information the user sends is only accessible by a range of users for whom it is intended. Many computer users assume that messages prepared and sent on the local network or the Internet, are read by the recipients to whom they were addressed. E-mail is like an open postcard. It can be read by anyone during its journey from sender to recipient. E-mail messages are very easy to intercept by malicious users. They often go through dozens of nodes (servers) in their way of transportation [6], [7]. Even if the message is sent to a local network a copy shall be kept on at least three machines: the sending computer, the computer of the recipient and the internal mail server. It is important to protect our data on our personal computer or office computer.

The protection of information is necessary for any of the following cases:

- protection from unauthorized use;
- protection against unauthorized modification;
- protection against unauthorized destruction of data.

Encryption involves converting data into a format that cannot be easily understood by others, but only by the creator of the data. When the documents are on an encrypted disk, only the user who has the correct key can view them. Personal data can be protected using permissions and encryption.

DATA ENCRYPTION SOFTWARE

There are a variety of software for data protection of passwords, emails, files and folders, whole hard disk and more. It is important to choose the right encryption software. It has to provide the desired protection [3], [5]. Encryption software should be convenient and easy to use. Some of these software products are discussed in this article:

- **CYPHERIX** is simple, easy to use encryption software that creates an encrypted virtual drive, provides password protection and hides any file or folder ensuring file encryption is automatic. Its powerful encryption ensures that only you can access your data. The free, fully-functional Cryptainer LE version uses a 128-bit implementation of the powerful Blowfish algorithm while the registered version Cryptainer ME offers a choice between a 448-bit implementation of the Blowfish and a 256-bit implementation of AES (Rijndael).
- **DataMotion Secure Mail Desktop** is achieved without complication. It protects all of your sensitive messages with military-grade encryption, and it gives customers

assurance that their private information is being handled with care. It works with popular email clients such as Outlook, it's intuitive for senders and recipients, and can be up and running in minutes with no outside IT support.

- **DESlock+ Pro** does it all. Full disk and removable media encryption protect laptop computers against unexpected events. File, folder and email encryption allow fully secure collaboration across complex work groups and team boundaries, with security policy enforced at all endpoints by the DESlock+ Enterprise Server. Full disk encryption - Fast transparent pre-boot security using FIPS validated 256 bit AES encryption.
- **IDOO File Encrypt Pro** is Free File Encryption and easy to use software to encrypt files by using a password. It is compatible with Windows OS 7/8/XP/Vista/2000. Using the advanced 256-bit AES encryption algorithm, it would protect the confidential data or private information from unauthorized access, and it is your best choice to prevent data breaches.
- **Nordic Information Security Group Flexcrypt** is a small software application that enables encryption and decryption of your emails. Flexcrypt is very easy to install and use. After installation, simply add the email addresses you wish to send and receive encrypted emails from. For each address, you must make up a password. This password is the key used in order to decrypt the message, thus, you must inform the receiver of the encrypted email of your chosen password.
- **SecureStar ShareCrypt** stores files encrypted on local disk, network shared folders, and file syncing cloud services. It provides user based access rights to folders and their content. Uses AES, Blowfish, RSA, SHA-2 Algorithms with 256 Bit Size Key.
- **WebMinds SensiGuard** is used for File and Folder Encryption. It uses AES Algorithm with 256 Bit Size Key and offers Instructional Video Support Features.
- **Symantec Drive Encryption** is expensive and powerful software product. It implements device Disk Encryption only using AES cryptographic Algorithm with 256 bit size key.
- **SOPHOS EndUser Data Suite** is freeware and simple to use. It provides Disk, File, Folder and Email Encryptions and uses SHA-2 Function and 128 Bit Size Key.
- **TrueCrypt Disk** is a freeware application. It creates a virtual encrypted disk within a file, or encrypts a partition or the entire storage device. TrueCrypt supports individual algorithms such as AES and Twofish. Five different combinations of cascaded algorithms are also available. The cryptographic hash functions that TrueCrypt uses are RIPEMD-160, SHA-512 and Whirlpool. This application supports parallelized encryption for multi-core systems and pipelined read/write operations.
- **AxCrypt** is a freeware software application designed for encryption and decryption of files. It uses an AES algorithm with a key length of 128 bits. AxCrypt creates an archive that contains additional metadata along with the encrypted data file. The original file is deleted after encryption.
- **ENTRUST Email Encryption** is a freeware application for Email Encryption. This software is, first and foremost, a secure service. Your private data will be on lockdown and you won't have to worry about bank account information or private medical data being divulged. But what helps this service become an even more desirable option is how simple it is to use.
- **Secude Finaily Secure Enterprise** was founded in 1996 out of a partnership between SAP AG and the Fraunhofer Institute, Germany. Provides Disk Encryption and Database Encryption and uses 128 Bit Size Key. It is free software and exploits AES, Blowfish and DES Algorithms.

- **PC Dynamics Safe House Personal Edition** provides total privacy and protection for your sensitive files and folders using passwords and strong encryption. SafeHouse features military-strength encryption, which is completely transparent to the way you work and compatible with all Windows applications. It uses AES and Blowfish Algorithms with 256 Bit Size Key.
- **Advanced Encryption Package Professional** is used for File and Folder Encryption Data. It supports Windows OS and allows compression and password access.

CRYPTOGRAPHY ALGORITHMS

Data encryption exploits some of the following algorithms [1], [4]:

- **RSA** is the most commonly used encryption and authentication algorithm, which was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. Briefly, the algorithm involves multiplying two large prime numbers and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded.
- **MD5** (Message Digest 5) is a one-way cryptographic hash function. MD5 performs many binary operations on the message to compute a 128-bit hash.
- **SHA-1** (Secure Hashing Algorithm 1). The Secure Hashing Standard is defined in FIPS PUB 180-1. SHA-1 can be used to produce a message digest for a given message. Essentially, this is a 160-bit number that represents the message. SHA-1 is used by Digital Signature Standard (DSS), which is a standard used for digitally signing documents or other data.
- **SHA-2** is a set of cryptographic hash functions designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 is a cryptographic hash function similar to MD5 and SHA-1. The hash functions generate a 224 bit, 256 bit, 384 bit or 512 bit message digest and accept a variable length input depending upon the function used. Unlike SHA-1, SHA-2 is a set of cryptographic hashing functions. SHA-2 comprises of SHA-224, SHA-256, SHA-384 and SHA-512.
- **Blowfish** is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.
- **DES** (Data Encryption Standard) encrypts blocks of size 64 bits. It was developed by IBM based on the cipher Lucifer under influence of the National Security Agency (NSA) and the design criteria for DES have not been published. It was standardized in 1977 by the National Bureau of Standards (NBS) today called National Institute of Standards and Technology (NIST). This is the most popular block cipher for most of the last 30 years. By far it is the best studied symmetric algorithm. Nowadays it is considered insecure due to the small key length of 56 bits. But 3DES yields very secure cipher, and is still widely used today.
- **AES/Rijndale** is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on the Rijndael cipher developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.
- **ElGamal**. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. The security of the RSA depends on the difficulty of factoring large integers; on

the difficulty of computing discrete logs in a large prime modulus. ElGamal has the disadvantage that the ciphered text is twice as long as the plain text.

- **HMAC** is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.

COMPARING DATA ENCRYPTION SOFTWARE

The paper presents a part of the existing commercial software for data encryption and their capabilities to facilitate user choice. The 11 criteria are used in the comparison:

- price;
- size of the encryption key;
- users for whom the software is intended;
- supported platforms;
- encryption methods;
- used encryption algorithms;
- encryption functions;
- additional opportunities to work with encrypted messages (in the case of supported to e-mail encryption function);
- files and folders encryption functions;
- disk encryption function;
- supported features.

Sixteen software products are presented are from the site http://encryption-software.findthebest.com/ [5]. Mainly free software and software that is affordable and best suits user needs for data protection is selected. A relational database was created to perform the comparison. There are select queries on giving criteria. Below we present the features for each of the encryption software to facilitate user choice.

Fig.1 shows the 16 discussed above programs for data encryption with their full names, sorted in ascending order of their prices. Presented is the method of payment of the price and the size of the used encryption key. Entrust and DataMotion Data Encryption Software don't use an encryption key because they are utilised for encryption of e-mail.

software_name	full name	price (in $)	payment	Bit Size Key
SECUDE	Secude Finaily Secure Enterprise	0		128
TRYE CRYPT	TryeCrypt Disk	0		256
AxCrypt	AxCrypt	0		128
CYPHERIX	Cypherix Le	0		128
ENTRUST	Entrust Email Encryption	0		0
SOPHOS	Sophos EndUser Data Suite	0		128
FLEXCRYPT	Nordic Information Security Group Flexcrypt 2010	4,72	annually	256
DataMotion	DataMotion Secure Mail Desctop	4,95	per user	0
CYPHERIX	Cypherix Me	30	per user	448
IDOO	IDOO File Encryption Pro	35	single payment	256
SensiGuard	WebMinds SensiGuard	39	annually	256
Advanced Encryption Package Professional	Inter Crypto Advanced Encryption Package	50	per user	80
SafeHouse Personal Edition	PC Dynamics Safe House Personal Edition	60	single payment	256
SecurStar	SecurStar Share Crypt	115	single payment	256
DESlock+	DESlock Pro	116	single payment	112
SYMANTEC	Symantec Drive Encryption	139	annually	256

Fig.1 Software Name, Full Name, Price and Bit Size Key

Figure 2 presents the algorithms for data encryption. All algorithms are considered as described above in the article. Examined software products do not use the DSA cryptography algorithm. An example of data encryption software that uses the DSA

algorithm is the Information Security Corporation, but it has other disadvantages such as costing $ 103; supports only Windows OS and does not support all Intended Users.

full name	price (in $)	AES	Blowfish	DES	HMAC	MD5	RSA	SHA-1	SHA-2	ElGamal
Finaily Secure Enterprise	0	☑	☑	☑	☐	☐	☐	☐	☐	☐
TryeCrypt Disk	0	☑	☑	☐	☐	☐	☐	☐	☐	☐
AxCrypt	0	☑	☐	☐	☑	☐	☐	☑	☐	☐
Cypherix Le	0	☐	☑	☐	☐	☐	☐	☐	☐	☐
Entrust Email Encryption	0	☐	☐	☐	☐	☐	☐	☐	☐	☐
Sophos EndUser Data Suite	0	☐	☐	☐	☐	☐	☐	☐	☑	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☐	☐	☐	☑	☐	☑	☑	☑
DataMotion Secure Mail Desctop	4,95	☑	☐	☑	☐	☐	☐	☐	☐	☐
Cypherix Me	30	☐	☑	☐	☐	☐	☐	☐	☐	☐
IDOO File Encryption Pro	35	☑	☐	☐	☐	☐	☐	☐	☐	☐
WebMinds SensiGuard	39	☑	☐	☐	☐	☐	☐	☐	☐	☐
Inter Crypto Advanced Encryption Package	50	☑	☑	☑	☐	☐	☑	☐	☐	☐
PC Dynamics Safe House Personal Edition	60	☑	☑	☐	☐	☐	☐	☐	☐	☐
SecurStar Share Crypt	115	☑	☑	☐	☐	☐	☑	☐	☑	☐
DESlock Pro	116	☑	☑	☑	☐	☐	☑	☑	☐	☐
Symantec Drive Encryption	139	☑	☐	☐	☐	☐	☐	☐	☐	☐

Fig.2 Encryption Algorithms

Intended Users of different data encryption software are shown in Fig. 3.

full name	price (in $)	Personal	Small- Medium	Large Business
Finaily Secure Enterprise	0	☐	☐	☑
TryeCrypt Disk	0	☑	☐	☐
AxCrypt	0	☑	☐	☐
Cypherix Le	0	☑	☐	☐
Entrust Email Encryption	0	☐	☐	☑
Sophos EndUser Data Suite	0	☐	☑	☑
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☑	☐
DataMotion Secure Mail Desctop	4,95	☐	☑	☑
Cypherix Me	30	☐	☐	☐
IDOO File Encryption Pro	35	☐	☐	☑
WebMinds SensiGuard	39	☑	☑	☐
Inter Crypto Advanced Encryption Package	50	☐	☑	☐
PC Dynamics Safe House Personal Edition	60	☐	☑	☐
SecurStar Share Crypt	115	☐	☐	☑
DESlock Pro	116	☐	☑	☐
Symantec Drive Encryption	139	☑	☑	☐

Fig.3 Intended Users

The supported platforms for each of the 16 data encryption software are shown in Fig. 4. Note that the Entrust Email Encryption Software does not support all operating systems, as it is only used for E-mail encryption. With the exception of Entrust and Data Motion Secure Mail Desktop all programs support Windows OS. None of the programs supports Mobile Platforms. For example Aloaha Secure Stick Data Encryption Software supports Mobile Platforms, but there are other disadvantages. It costs $ 140 and does not support the File / Folder Encryption Features.

full name	price (in $)	Linux	Mac	Online	Windows	Mobile
Finaily Secure Enterprise	0	☐	☐	☐	☑	☐
TryeCrypt Disk	0	☑	☑	☐	☑	☐
AxCrypt	0	☐	☐	☐	☑	☐
Cypherix Le	0	☐	☐	☐	☑	☐
Entrust Email Encryption	0	☐	☐	☐	☐	☐
Sophos EndUser Data Suite	0	☑	☑	☐	☑	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☐	☐	☐	☑	☐
DataMotion Secure Mail Desctop	4,95	☐	☐	☑	☐	☐
Cypherix Me	30	☐	☐	☑	☑	☐
IDOO File Encryption Pro	35	☐	☐	☐	☑	☐
WebMinds SensiGuard	39	☐	☐	☑	☑	☐
Inter Crypto Advanced Encryption Package	50	☐	☐	☐	☑	☐
PC Dynamics Safe House Personal Edition	60	☐	☐	☐	☑	☐
SecurStar Share Crypt	115	☐	☐	☐	☑	☐
DESlock Pro	116	☐	☐	☐	☑	☐
Symantec Drive Encryption	139	☑	☑	☑	☑	☐

Fig.4 Supported Platforms

Fig. 5 presents the supported encryption methods. It is noted that with the exception of Sophos EndUser Data Suite Software all support symmetric encryption methods. Flexcrypt Data Encryption Software supports symmetric and asymmetric encryption methods, and Hash Function.

full name	price (in $)	Asymmetric Method	Hashing	Symmetric Method
Finaily Secure Enterprise	0	☐	☐	☑
TryeCrypt Disk	0	☐	☐	☑
AxCrypt	0	☐	☑	☑
Cypherix Le	0	☐	☐	☑
Entrust Email Encryption	0	☐	☐	☑
Sophos EndUser Data Suite	0	☐	☑	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☑	☑
DataMotion Secure Mail Desctop	4,95	☐	☐	☑
Cypherix Me	30	☐	☐	☑
IDOO File Encryption Pro	35	☐	☐	☑
WebMinds SensiGuard	39	☐	☐	☑
Inter Crypto Advanced Encryption Package	50	☑	☐	☑
PC Dynamics Safe House Personal Edition	60	☐	☐	☑
SecurStar Share Crypt	115	☑	☑	☑
DESlock Pro	116	☑	☑	☑
Symantec Drive Encryption	139	☐	☐	☑

Fig. 5 Supported Encryption Methods

The supported features for each encryption software are presented in Fig. 6. We can conclude that almost all programs support encryption of files and folders. Only Finaily Secure Enterprise Software supports database encryption. Among all 16 data encryption software Sophos and Flexcrypt are the best at this parameter. They support disk encryption, files and folders encryption and e-mail encryption.

full name	price (in $)	Disk Encryption	Email Encryption	File/Folder Encryption	Database Encryption
Finaily Secure Enterprise	0	☑	☐	☐	☑
TryeCrypt Disk	0	☑	☐	☐	☐
AxCrypt	0	☐	☐	☑	☐
Cypherix Le	0	☑	☑	☑	☐
Entrust Email Encryption	0	☐	☑	☐	☐
Sophos EndUser Data Suite	0	☑	☑	☑	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☑	☑	☐
DataMotion Secure Mail Desctop	4,95	☐	☑	☐	☐
Cypherix Me	30	☑	☑	☑	☐
IDOO File Encryption Pro	35	☐	☐	☑	☐
WebMinds SensiGuard	39	☐	☐	☑	☐
Inter Crypto Advanced Encryption Package	50	☐	☐	☑	☐
PC Dynamics Safe House Personal Edition	60	☐	☐	☑	☐
SecurStar Share Crypt	115	☑	☐	☐	☐
DESlock Pro	116	☑	☑	☑	☐
Symantec Drive Encryption	139	☑	☐	☐	☐

Fig.6 Supported Primary Functions

Because out of the 16 products only 4 supports email encryption a list of their features was created with a select query sorting by price of the products. They are represented in Fig. 7.

full name	price (in $)	Client Encryption	Gateway Encryption	Mobile Email	Password Recovery	Manageable Permissions	Transparent Reading
Entrust Email Encryption	0	☑	☑	☐	☐	☐	☑
Sophos EndUser Data Suite	0	☑	☑	☐	☐	☑	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☐	☐	☐	☐	☐
DataMotion Secure Mail Desctop	4,95	☑	☑	☑	☑	☐	☐

Fig.7 Supported Email Encryption Features

Fig. 8 presents supported file and folder encryption features. The features for file and folder encryptions are: compression, document sharing, file shredding, file/folder hiding,

password access, password recovery and USB key (shown in Fig. 8). We note that only two programs support password recovery. These are AxCrypt and Symantec Drive Encryption Software.

full name	price (in $)	Compression	Document Sharing	File Shredding	File/ Folder Hiding	Password Access	Password Recovery	USB Key
Finaily Secure Enterprise	0	☐	☐	☐	☑	☑	☐	☐
TryeCrypt Disk	0	☐	☐	☐	☐	☐	☐	☐
AxCrypt	0	☑	☑	☑	☑	☑	☑	☐
Cypherix Le	0	☐	☐	☐	☑	☑	☐	☑
Entrust Email Encryption	0	☐	☐	☐	☐	☐	☐	☐
Sophos EndUser Data Suite	0	☐	☐	☑	☐	☐	☐	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☑	☑	☐	☑	☐	☐
DataMotion Secure Mail Desctop	4,95	☐	☐	☐	☐	☐	☐	☐
Cypherix Me	30	☐	☐	☐	☑	☐	☐	☐
IDOO File Encryption Pro	35	☐	☑	☑	☐	☑	☐	☐
WebMinds SensiGuard	39	☑	☐	☑	☑	☐	☐	☑
Inter Crypto Advanced Encryption Package	50	☑	☐	☐	☐	☑	☐	☑
PC Dynamics Safe House Personal Edition	60	☐	☐	☐	☑	☑	☐	☑
SecurStar Share Crypt	115	☐	☑	☐	☑	☐	☐	☐
DESlock Pro	116	☐	☑	☐	☐	☐	☐	☑
Symantec Drive Encryption	139	☐	☐	☐	☐	☐	☑	☐

Fig.8 Support File /Folder Encryption Features

From the presented data encryption software only 5 products allow to choose the cryptographic algorithm. The supported disk encryption features are presented in Fig.9.

full name	price (in $)	Backup	Hidden Volume	Password Access	Pre-Boot Authentication	Whole Disk Encryption	Algorithm Choices
Finaily Secure Enterprise	0	☐	☐	☐	☑	☐	☑
TryeCrypt Disk	0	☐	☑	☑	☑	☐	☑
AxCrypt	0	☐	☐	☐	☐	☐	☐
Cypherix Le	0	☐	☐	☑	☐	☐	☑
Entrust Email Encryption	0	☐	☐	☐	☐	☐	☐
Sophos EndUser Data Suite	0	☑	☑	☑	☑	☐	☑
Nordic Information Security Group Flexcrypt 2010	4,72	☐	☐	☑	☐	☐	☐
DataMotion Secure Mail Desctop	4,95	☐	☐	☐	☐	☐	☐
Cypherix Me	30	☐	☑	☐	☐	☐	☑
IDOO File Encryption Pro	35	☐	☐	☐	☐	☐	☐
WebMinds SensiGuard	39	☐	☐	☐	☐	☐	☐
Inter Crypto Advanced Encryption Package	50	☐	☐	☐	☐	☐	☐
PC Dynamics Safe House Personal Edition	60	☑	☑	☐	☐	☐	☐
SecurStar Share Crypt	115	☑	☐	☐	☑	☑	☐
DESlock Pro	116	☐	☐	☐	☑	☑	☐
Symantec Drive Encryption	139	☑	☑	☐	☑	☑	☐

Fig.9 Supported Disk Encryption Features

For all data encryption software, along with the features user support is also very important. Fig. 10 shows that no one of the examined software has with full support. Almost all software uses phone support, FAQ and Data Sheet support. Only TryeCrypt Data Encryption provides a Forum for Online support and own Self Help. Sophos also offers four types of support Data Sheet, FAQ, Phone support and Installation Help.

full name	price (in $)	Data Sheet	FAQ	Installation Help	Instructional Video	Phone support	Self Help	Forum
Finaily Secure Enterprise	0	☐	☐	☐	☐	☑	☐	☐
TryeCrypt Disk	0	☑	☑	☐	☐	☐	☑	☑
AxCrypt	0	☐	☑	☑	☐	☑	☐	☐
Cypherix Le	0	☐	☑	☑	☐	☐	☐	☐
Entrust Email Encryption	0	☐	☐	☐	☐	☑	☐	☐
Sophos EndUser Data Suite	0	☑	☑	☑	☐	☑	☐	☐
Nordic Information Security Group Flexcrypt 2010	4,72	☑	☐	☐	☐	☐	☐	☐
DataMotion Secure Mail Desctop	4,95	☑	☑	☐	☐	☑	☐	☐
Cypherix Me	30	☐	☑	☑	☐	☐	☐	☐
IDOO File Encryption Pro	35	☐	☐	☐	☐	☐	☐	☐
WebMinds SensiGuard	39	☐	☑	☐	☑	☐	☐	☐
Inter Crypto Advanced Encryption Package	50	☐	☐	☐	☐	☐	☐	☐
PC Dynamics Safe House Personal Edition	60	☑	☑	☐	☑	☐	☐	☐
SecurStar Share Crypt	115	☐	☑	☐	☑	☑	☐	☐
DESlock Pro	116	☑	☐	☐	☐	☑	☐	☐
Symantec Drive Encryption	139	☑	☐	☐	☐	☑	☐	☐

Fig.10 User Support Features

CONCLUSION

1. In conclusion it can be said that out of 16 data encryption software according Privacy PC [2], the following 4 software products are the best (Table 1):

Table 1: Best Encryption Software Review

№	Software Name	Price	Usability	Features	Efficiency	Support	Overall
1	True Crypt	Free	80%	100%	100%	60%	85%
2	Safe House Personal Edition	$60	90%	80%	80%	80%	83%
3	Sensi Guard	$39	80%	70%	80%	80%	78%
4	Advanced Encryption Package Proffesional	$50	70%	80%	80%	70%	75%

Each data encryption software package has advantages and disadvantages.

2. Table 2 presents the main advantages and disadvantages of the compared free data encryption software.

Table 2: Free data encryption software

Secude Finaily Secure Enterprise	TryeCrypt Disk	AxCrypt	Cypherix Le	Entrust Email Encryption	Sophos EndUser Data Suite
Advantages					
Provides choices on cryptographic algorithm	Use 256 bit size key	Provides compression, document sharing, file shredding, file/ folder hiding, password access, password recovery encryption features	Provides choices on cryptographic algorithm	Use email encryption	Use email encryption
Supported database encryption primary function	Supported Windows, Linux and Mac OS	Use Hashing and symmetric cryptographic methods	Support file/ folder hiding, password access and USB key	Support Transparent Reading Email Features.	Supported Windows, Linux and Mac OS
Use AES, Blowfish and DES cryptographic algorithms	Use Forum and Self Help Support Features	Use AES, HMAC and SHA-1 cryptographic Algorithms	Provides installation help	Used for large business	The most support features:Data Sheet, FAQ, Installation help and phone support
Disadvantages					
provides phone support only	Use personal intended users only	No support disk encryption features	Use only Blowfish cryptographic algorithms	No support operation system and cryptographic algorithms	No support symmetric encryption methods
Support Windows OS only	Use Disk encryption only	Use personal intended users only	Use symmetric cryptographic methods only	No support File/ Folder Encryption Features	Use only SHA-2 cryptographic algorithms

3. Table 3 presents the main advantages and disadvantages of the compared paid data encryption software.

Table 3: Paid data encryption software

Flexcrypt	DataMotion	Cypherix Me	IDOO	SensiGuard	Advanced Encryption Package Professional	Safe House Personal Edition	SecurStar Share Crypt	DESlock Pro	Symantec
Advantages									
- use email encryption; - provides Disk, Email and File/ Folder Encryption; - supported ElGamal and MD5 cryptographic algorithms	- is quick and easy to use; - support mobile Email and password recovery; - use email encryption; work on Smartphone platform	- provides choices on cryptographic algorithm; - use 448 Bit size key	- use 256 bit size key; - low price; - allows document sharing, file shredding and password access	- use 256 bit size key; - allows compression, USB key, file shredding and file/ folder hiding encryption features; - use instructional video support features	- allows compression , password access and USB key encryption features; - support symmetric and asymmetric cryptography methods	-support Backup disk encryption features; - allows file/folder hiding, password access and USB key encryption features; - use 256 bit size key	-support Asymmetric, Symmetric Methods and Hashing; - support Backup disk encryption features	-supports all encryption methods; - support disk, email and file/ folder encryption	-support Backup, Hidden Volume, Pre-Boot Authentication, Whole disk encryption; - support Backup disk encryption features
Disadvantages									
-provides Client Email Encryption only; - support data sheet features only	-no use bit size key; - does not support file/folder encryption features	-no support encryption methods; - no support Intended users	-no Support Features; no support disk encryption features; - use only AES cryptographic algorithms	-use only AES cryptographic algorithms and only Online encryption; - no support disk encryption	-no support features; -support Windows OS only; - no support disk encryption features	-support symmetric and cryptography methods only; - support Windows OS only	-is expensive; - support Windows OS only	-is expensive; - support Windows OS only	-the most expensive of issue; - use only AES cryptographic algorithms

"The present document has been produced with the financial assistance of the European Social Fund under Operational Programme "Human Resources Development". The contents of this document are the sole responsibility of the "Angel Kanchev" University of Ruse and can under no circumstances be regarded as reflecting the position of the European Union or the Ministry of Education and Science of Republic of Bulgaria."

Project № BG051PO001-3.3.06-0008 "Supporting Academic Development of Scientific Personnel in Engineering and Information Science and Technologies"

REFERENCES

[1] G. Brassard. Modern Cryptology - A Tutorial. Lecture Notes in Computer Science, vol. 325, Springer-Verlag, 1988.

[2] Privacy PC, 2014 Best Encryption software reviews, 2014. http://privacy-pc.com/encryption-software-review, [date accessed 6th January 2014, 21:30].

[3] Ramesh Natarajan, Top 5 Best Free File Encryption Software for Windows, 2013 http://www.top5freeware.com/file-encryption-software-for-windows [date accessed 22th Marth 2014, 19:20].

[4] Swinton Manchester, Cryptography world, http://www.cryptographyworld.com/algo.htm [date accessed 13th Febryary 2014, 20:30].

[5] Compare Encryption Software, http://encryption-software.findthebest.com/, [date accessed 7th November 2013, 16:00].

[6] Мерки за повишаване на мрежовата сигурност, http://193.192.57.240/po/courses/problemni/mrezi/HTML/section5_theme3.html [date accessed 25th January 2014, 22:00].

[7] Компютърни мрежи. Електронен учебен курс. Мерки за повишаване на мрежовата сигурност, http://networks.hit.bg/map.html [date accessed 17th December 2013, 22:30].

CONTACT ADDRESS
Pr. Assist. Victoria Rashkova, PhD
Department of Informatics and Information Technologies
Faculty of Natural Sciences and Education
Angel Kanchev University of Ruse
8 Studentska Str., 7017 Ruse, Bulgaria
Phone: (++359 82) 888 214
E-mail: vkr@ami.uni-ruse.bg

СОФТУЕР ЗА КРИПТИРАНЕ НА ДАННИ

Виктория Рашкова

Русенски университет "Ангел Кънчев"

Резюме: *Основен проблем за всички потребители е защитата на личните им данни. В статията са представени основните криптографски алгоритми. Представени са различни софтуерни продукти за криптиране на данни, избрани от [4]. Създадена е релационна база данни за съпоставка между тях по следните показатели: цена, размер на ключа, платформа, използван метод на криптиране, потребители, за които е предназначен, възможности, поддръжка. Представени са предимствата и недостатъците на избрания софтуер, за улесняване избора на потребителя.*

Ключови думи: *криптиране, декриптиране, размер на криптографски ключ, защита на данните, софтуер за криптиране.*

Requirements and guidelines for the authors - "Proceedings of the Union of Scientists - Ruse" Book 5 Mathematics, Informatics and Physics

The Editorial Board accepts for publication annually both scientific, applied research and methodology papers, as well as announcements, reviews, information materials, adds. No honoraria are paid.

The paper scripts submitted to the Board should answer the following requirements:

1. Papers submitted in English are accepted. Their volume should not exceed 8 pages, formatted following the requirements, including reference, tables, figures and abstract.

2. The text should be computer generated (MS Word 2003 for Windows or higher versions) and printed in one copy, possibly on laser printer and on one side of the page. Together with the printed copy the author should submit a disk (or send an e-mail copy to: vkr@ami.uni-ruse.bg).

3. Compulsory requirements on formatting:

- font - Ariel 12;
- paper Size - A4;
- page Setup - Top: 20 mm, Bottom: 15 mm, Left: 20 mm, Right: 20mm;
- Format/Paragraph/Line spacing - Single;
- Format/Paragraph/Special: First Line, By: 1 cm;
- *Leave a blank line under Header - Font Size 14;*
- Title should be short, no abbreviations, no formulas or special symbols - Font Size 14, centered, Bold, All Caps;
- *One blank line - Font Size 14;*
- Name and surname of author(s) - Font Size: 12, centered, Bold;
- *One blank line - Font Size 12*;
- Name of place of work - Font Size: 12, centered;
- *One blank line;*
- abstract – no formulas - Font Size 10, Italic, 5-6 lines ;
- keywords - Font Size 10, Italic, 1-2 lines;
- *one blank line;*
- text - Font Size 12, Justify;
- references;
- contact address - three names of the author(s) scientific title and degree, place of work, telephone number, Email - in the language of the paper.

4. At the end of the paper the authors should write:

- The title of the paper;
- Name and surname of the author(s);
- abstract; keywords.

Note: The parts in item 4 should be in Bulgarian and have to be formatted as in the beginning of the paper.

5. All mathematical signs and other special symbols should be written clearly and legibly so as to avoid ambiguity when read. All formulas, cited in the text, should be numbered on the right.

6. Figures (black and white), made with some of the widespread software, should be integrated in the text.

7. Tables should have numbers and titles above them, centered right.

8. Reference sources cited in the text should be marked by a number in square brackets.

9. Only titles cited in the text should be included in the references, their numbers put in square brackets. The reference items should be arranged in alphabetical order, using the surname of the first author, and written following the standard. If the main text is in Bulgarian or Russian, the titles in Cyrillic come before those in Latin. If the main text is in English, the titles in Latin come before those in Cyrillic. The paper cited should have: for the first author – surname and first name initial; for the second and other authors – first name initial and surname; title of the paper; name of the publishing source; number of volume (in Arabic figures); year; first and last page number of the paper. For a book cited the following must be marked: author(s) – surname and initials, title, city, publishing house, year of publication.

10. **The author(s) and the reviewer, chosen by the Editorial Board, are responsible for the contents of the materials submitted**.

Important for readers, companies and organizations

1. Authors, who are not members of the Union of Scientists - Ruse, should pay for publishing of materials.

2. Advertising and information materials of group members of the Union of Scientists – Ruse are published free of charge.

3. Advertising and information materials of companies and organizations are charged on negotiable (current) prices.

Editorial Board

ISSN 1314-3077