Datarizer

Datarizer

mecryption

Version 1

Table of Contents

Section Page

1

Mecryption

Application Icon

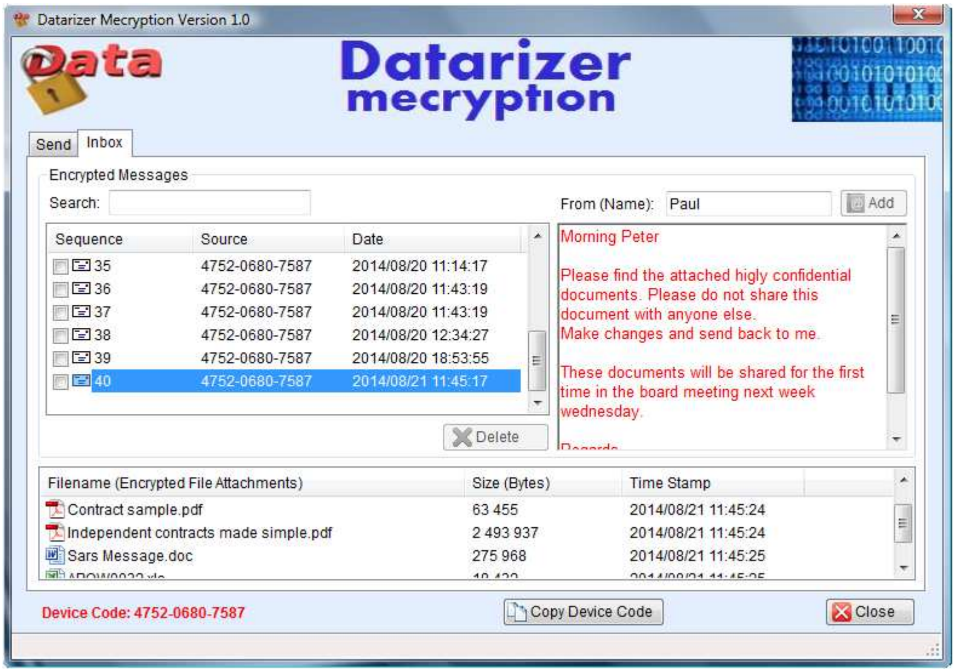
Overview

a) What is Datarizer mecryption?

Datarizer mecryption is a software program or application that encrypts messages and files intended to be transmitted from one device (computer) to another across the internet securely using Advanced Encryption Standard (AES) of 128 bit encryption.

It is a simple application that does this without the use of emails and ISP's. Encrypted data is transmitted from one computer to the other. The sending computer encrypts the data and transmits it to the recipient computer. The recipient computer saves the encrypted data on the hard drive in encrypted format. Data is kept in the encrypted format until the user is ready to use it.

If you can open a computer file and send emails, you can use this application. It is as simple as sending a text message on a smart phone.



Datarizer Mecryption Version 1.0

From (Name): Paul

Sequence	Source	Date
□ 35	4752-0680-7587	2014/08/20 11:14:17
□ 36	4752-0680-7587	2014/08/20 11:43:19
□ 37	4752-0680-7587	2014/08/20 11:43:19
□ 38	4752-0680-7587	2014/08/20 12:34:27
□ 39	4752-0680-7587	2014/08/20 18:53:55
□ 40	4752-0680-7587	2014/08/21 11:45:17

Morning Peter

Please find the attached higly confidential documents. Please do not share this document with anyone else.
Make changes and send back to me.

These documents will be shared for the first time in the board meeting next week wednesday.

Filename (Encrypted File Attachments)	Size (Bytes)	Time Stamp
Contract sample.pdf	63 455	2014/08/21 11:45:24
Independent contracts made simple.pdf	2 493 937	2014/08/21 11:45:24
Sars Message.doc	275 968	2014/08/21 11:45:25

Device Code: 4752-0680-7587

b) What is data Encryption?

Encryption is the process of deciphering electronic data using an encryption standard such as AES, DES, RSA or SHA1 etc. It is the process of removing the "*meaning*" from electronic data and make it "*meaningless*" and render it useless to be used for anything. This is the only way to protect electronic data:-

- on the internet (Wifi, Bluetooth, Satellite, LAN and other networks),
- on a disk or other data mediums.

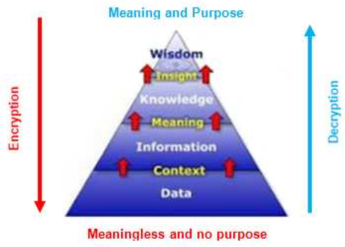
All internet traffic data can be intercepted and encryption techniques are the only protection security means available to protect data. Data saved on a device (computer, mac, smartphone) disk can be stolen using advanced botnets and again, encryption is the only protection available. All the emails can be read by the ISP. Nothing is really secure unless wrapped by encryption.

It is important to note that encrypted data can also be intercepted. The only difference or advance it that it all useless and meaningless, it cannot be used for anything. In other words, encryption does not protect data, but the "*meaning*" thereof.

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 ('*denies the meaning*') to the interceptor.

Encryption means that, what one wants to keep secretive, confidential and private remains just that.

Decryption is the reverse process of encryption.



Purpose of Cryptography

c) Why?

The problem started back in 2001 during the 9/11 event. The birth of terrorism brought this upon all of us. Today, each and every individual is surveyed by governments in an effort to track and trace terrorism activities.

Hacking, phishing and advanced botnets started appearing on the forefront. This was not a problem pre-2000 era. No one is immune from this problem as the cyberworld is connected from all angles. Devices no longer operate fully independently. Connectivity is required all the time. Everyone longing for data privacy should compute carefully with this knowledge in mind.

Governments, cyber security experts, hackers and other computer literate individuals understands that:-

- correct data or word with meaning, could be a password to launch a missile from a bunker,
- unauthorised access into a database could destroy a bank, business, organization or shutdown the entire electricity grid or telecommunications or stock market.

The globe depends on data and it must be protected because it could unleash unimaginable chaos we have not seen before.

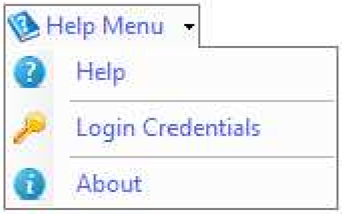
d) Information Security

Information security is a difficult task and hence the companies are employing their own information security experts. This area has got a massive skills shortage.

For more information visit the following link:-

- http://www.tcij.org/
- http://files.gendo.nl/Books/Information_Security_for_Journalists_v1.01.pdf

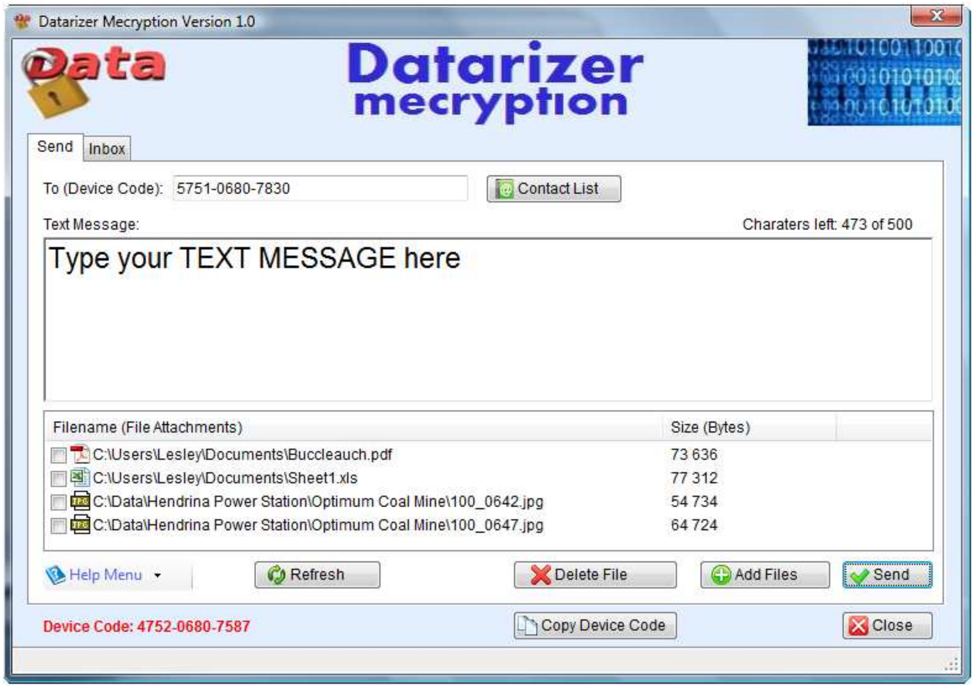
2



Bottom Left Menu

Datarizer mecryption User Interface

Datarizer mecryption has a single window interface for simplicity. Each application has a unique code called "***Device Code***". It is indicated in red at the bottom left corner. The Device Code must be used to transmit from one computer to another, like an email address. No email addresses, no Internet Service Providers, no registrations. It is all machines, sender and recipient.



To (Device Code): 5751-0680-7830

Text Message:

Charaters left: 473 of 500

Type your TEXT MESSAGE here

Filename (File Attachments)	Size (Bytes)
□ C:\Users\Lesley\Documents\Buccleauch.pdf	73 636
□ C:\Users\Lesley\Documents\Sheet1.xls	77 312
□ C:\Data\Hendrina Power Station\Optimum Coal Mine\100_0642.jpg	54 734
□ C:\Data\Hendrina Power Station\Optimum Coal Mine\100_0647.jpg	64 724

Device Code: 4752-0680-7587

Initially, the user is prompted to select a password or no password. Please select to use a password, unless:-

- Your computer is password protected,
- You are the only user on this device,
- Computer is always in your possession.

The good advice is always to have a password.

Password and security question can be changed anytime using the menu. If one forgets the **password and security answer**, one is in big trouble because the application is independent of humans, it is all machines. If you forget the password only, no problem, the device will reset you using the security question and answer.

Datarizer Mecryption takes care of public keys, private keys so that the user does not need to worry. Type message and attach files and click ***Send*** button, that is all.

It is possible to send a text message only without any file attachments and vice versa. A text message should not be longer than 500 characters.

The word "**mecryption**" is derived from **me**ssage/en**cryp**tion/decryp**tion**.

3

How does it Work?

a) Advanced Encryption Standard (AES 128 bit)

Datarizer mecryption applied AES 128 bit standard to encrypt data.

The Advanced Encryption Standard (AES), the symmetric block cipher ratified as a standard by National Institute of Standards and Technology of the United States (NIST). It is open and transparent than its predecessor, the aging Data Encryption Standard (DES). This process won praise from the open cryptographic community, and helped to increase confidence in the security of the winning algorithm.

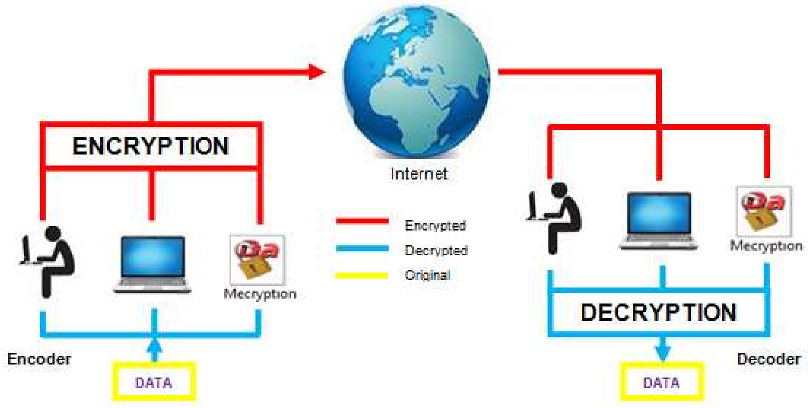
AES has 128, 192 and 254 bit keys which means, currently the known computational power will take **100** years to decrypt 128 bit without the appropriate key (commonly known as private key), whereas 254 bit will take **500** years. So, as far as we know today, it is practically impossible to break this encryption algorithm.

This is a brief explanation on the surface, underneath the AES algorithm is much more complex than explained above.

b) 2^3 Information Security Protection

Datarizer mecryption utilises a ***cube*** information security protection system that will be explained in detail shortly. The cube is made up of two (2) computers that must transmit data and this is a function (*f*) of:-

1. *User*,
2. *Device (computer),*
3. *Datarizer mecryption software.*



If any of the three input requirements is missing, Decryption process will fail. This function is build on top of the already existing and secure AES encryption algorithm which is applied by Datarizer mecryption software.

<u>*User*</u>

Users device or computer is password protect on OS level. In addition, Datarizer mecryption has a password before one gets to retrieve or send data.

One needs to get through two passwords before access to the encrypted data on a local hard drive. All the encrypted data is not saved on local drive folder but resides www.comodo.com

inside a database which has its own password which is unknown to the owner of the device. If one gets past this point, one will be confronted with encrypted data. Encrypted data is kept inside the database on a local hard drive.

Device (computer)

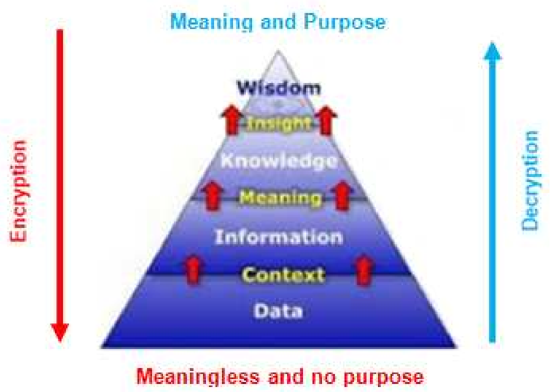
Each device is unique and has own ***Device Code***. The Device Code from the Decoder is used in the encryption function to encrypt and also transmit encrypted data to the correct device. The transmitted encrypted data cannot be retrieved by any other device but the one used in the cube encryption function.

If encrypted data is stolen from one device and transferred to another device also running Datarizer mecryption. Decryption process fails because Datarizer mecryption will detect device mismatch.

Datarizer mecryption software

Datarizer mecryption applies the AES algorithm and the cube function to create secure keys which are ever changing.

Data that is encrypted using Datarizer mecryption needs the same software to decrypt the data. The encrypted data is tied down to the two devices in one direction only. Even the device that was used to encrypt the data will not be able to decrypt the same data if encrypted data was transferred by other means back to the encoder. This is one directional and meant for one device (decoder) of which the Device Code was used in the encryption formula.



Encrypted data is not saved in file folder as such which is accessible. Encrypted data is saved in a database on a local drive which increases security.

Datarizer mecryption does not decrypt data until the user requests to see the data. The software merely retrieved the encrypted data and save it in the same encrypted format in a local database.

The formulae for the Private Key and Initiation Vector are as follows:-

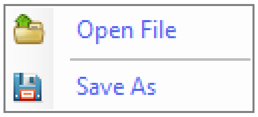
[Private Key = ƒ(*User*, *Device*, *mecryption*)]^2

[Initiation Vector = ƒ(*User*, *Device*, *mecryption*)]^2

There is a tradeoff between encryption and performance. Datarizer mecryption is ready to upgrade to 192 bit but for now, we shall stick to 128 bit and have a bit of performance improvement. After, all humans do not live for more than 100 years.

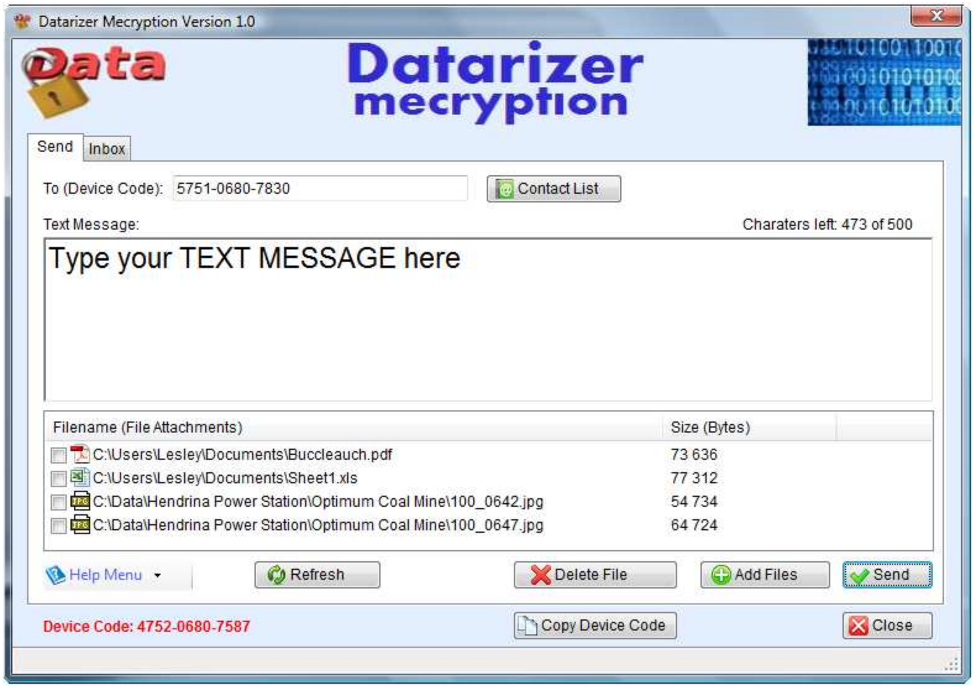
Datarizer mecryption software is code signed by a digital certificate from www.comodo.com.

4



File Attachments Right click menu

How to Send and Receive messages?



To (Device Code): 5751-0680-7830

Text Message:

Charaters left: 473 of 500

Type your TEXT MESSAGE here

Filename (File Attachments)	Size (Bytes)
□ C:\Users\Lesley\Documents\Buccleauch.pdf	73 636
□ C:\Users\Lesley\Documents\Sheet1.xls	77 312
□ C:\Data\Hendrina Power Station\Optimum Coal Mine\100_0642.jpg	54 734
□ C:\Data\Hendrina Power Station\Optimum Coal Mine\100_0647.jpg	64 724

Device Code: 4752-0680-7587

a) Pre-requisites

Before encrypted messages can be send from one computer to another, the following pre-requisite must be met:-

1. Both computers (sender^{encoder} and receiver^{decoder}) must have Datarizer mecryption application installed.
2. Internet connection.

Internet connection is required only to send and receive encrypted data. It is not required to decrypt and read messages in the Inbox as this data resides on the local hard drive in encrypted format.

b) Procedure to send Encrypted Messages

1. Launch Datarizer mecryption.
2. Type the ***Device Code*** of the receiving computer.
3. Type Text Message, Attach files and click ***Send*** button. or
   a. Type Text Message and click ***Send*** button. or
   b. Attach file/s and click ***Send*** button. (Encryption process starts)
4. That is all.

c) Procedure to receive Encrypted Messages

1. Launch Datarizer mecryption.
2. Go to Inbox tab. All messages and files are still in encrypted format.
3. Click on a message, Text Message will be decrypted and shown. Attached filed will be indicated (still encrypted format).
4. Double click or Right click and select ***Open File*** to open the attached file. (Decryption process starts).
5. Right click file attached and select ***Save As*** to save the file (decrypted file).

5

Contact Us

Company Name:	Datarizer Inc.
Website:	http://www.datarizer.co.za
E-mail:	info@datarizer.co.za
Contact:	Lesley Baloyi
Cell:	+27 72-625-7662
Fax number:	+27 86-688-5128

Datarizer Inc. can develop a customized software application for personal use to protect data on your computer. Encrypt all your confidential files on your file folders. If you get phished or your computer is stolen, your data cannot be used for any purpose.

NB: Encrypted data must also be backed up. Datarizer mecryption is a bit tricky in this area due to security design features.