

One distributed key creates an infinite number of one time pads for all network security controls : a virtual framework that is virtually manufactured and provisioned.

# Whitenoise Technologies

*Total Information Security*



[www.wnlabs.com](http://www.wnlabs.com)

[abrisson@wnlabs.com](mailto:abrisson@wnlabs.com)

June 15, 2014

## INSTALLATION AND USE INSTRUCTIONS FOR THE WHITENOISE EMAIL ATTACHMENT ENCRYPTOR

Recently Google announced that they are providing a free plug-in to encrypt emails on Gmail to help you with privacy.

Whitenoise Labs believes that encrypting entire emails is not particularly functional since all the formatting associated with the email becomes a crib. A crib is information that is used to break encryption down.


We are providing you the Whitenoise Email Attachment Encryptor for free and as a public service. You will encrypt the file you wish to send to another party. Then email the other party and send the encrypted file as an attachment. Voila – there is no crib material.

The Google plug-in may also have a problematic key exchange.

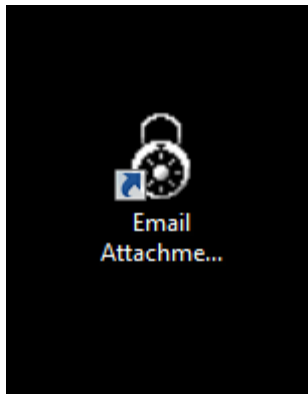
With this simple Whitenoise utility you will perturb (make unique) a Whitenoise key that is greater than 250,000 bits in strength by using two pass phrases.

NOTE: the resultant key will only be as strong as the pass phrases you choose. People as a habit choose poor passwords. The inclusion of the second pass phrase will increase the strength of the resultant encryption. Note however, you have never transmitted these pass phrases electronically so it makes the job of the bad guys virtually impossible. Choose longer words and include a number and non-alpha numeric symbol if possible. Enjoy your privacy.

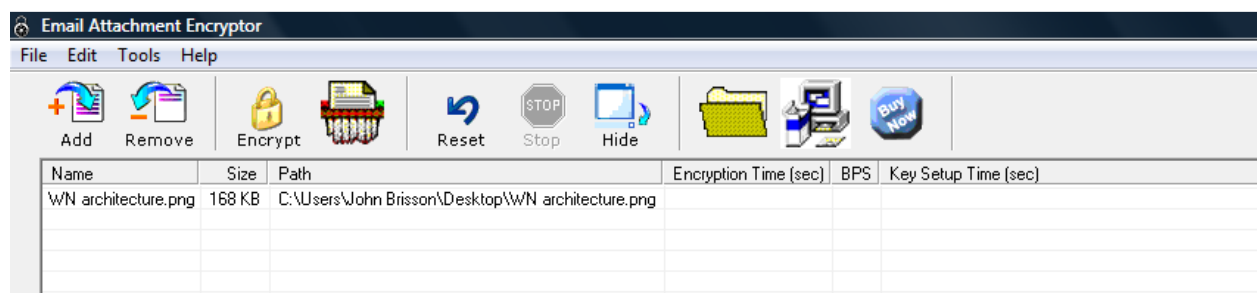
1. Download the Whitenoise Email Attachment Encryptor zip file.
2. Unzip the file to your desktop.
3. Go into the Email folder and click on EASETUP. It will take just moments to install.

 EASETUP	8/28/2006 9:16 PM	Application	699 KB
---	-------------------	-------------	--------

You are ready to go. You don't even need to reboot.

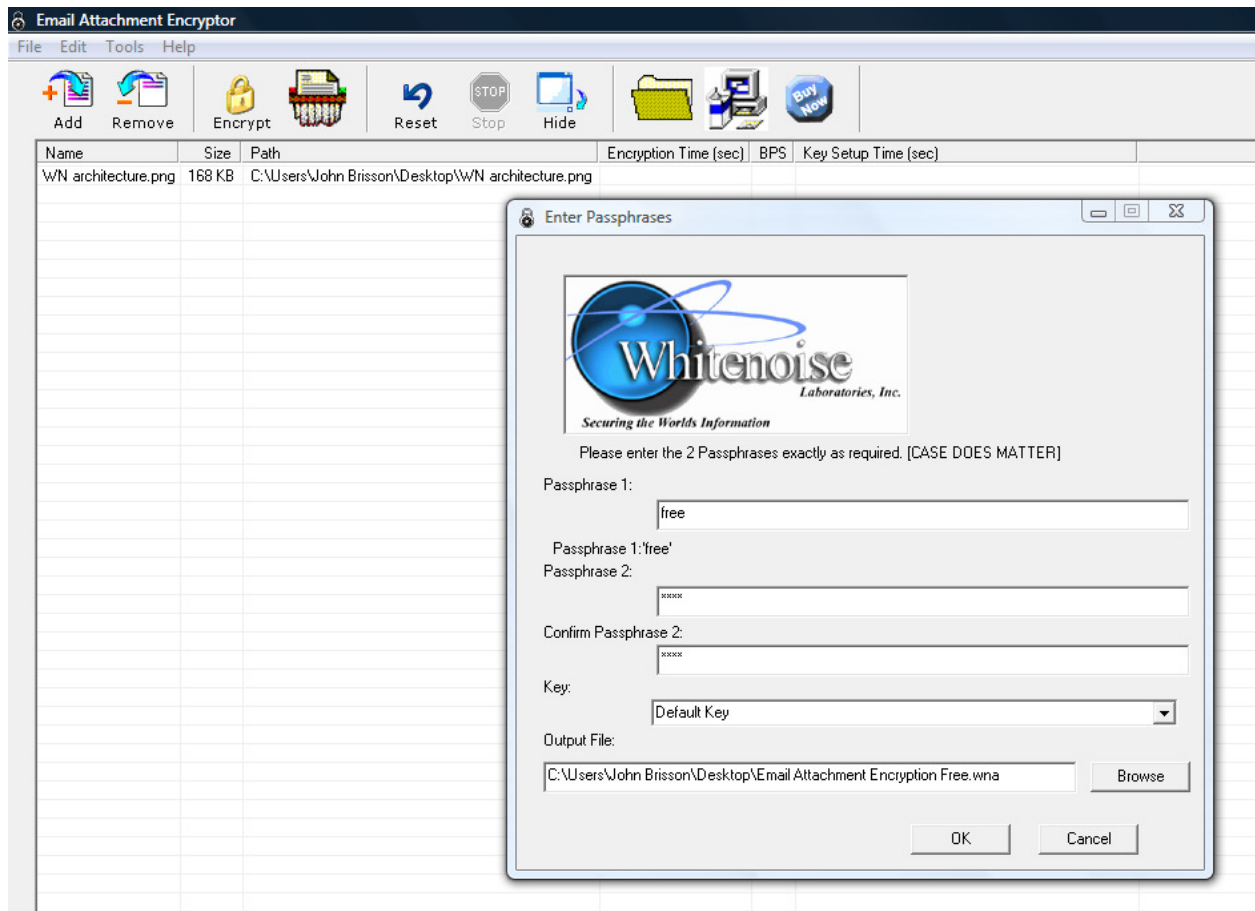


Click on the application icon.

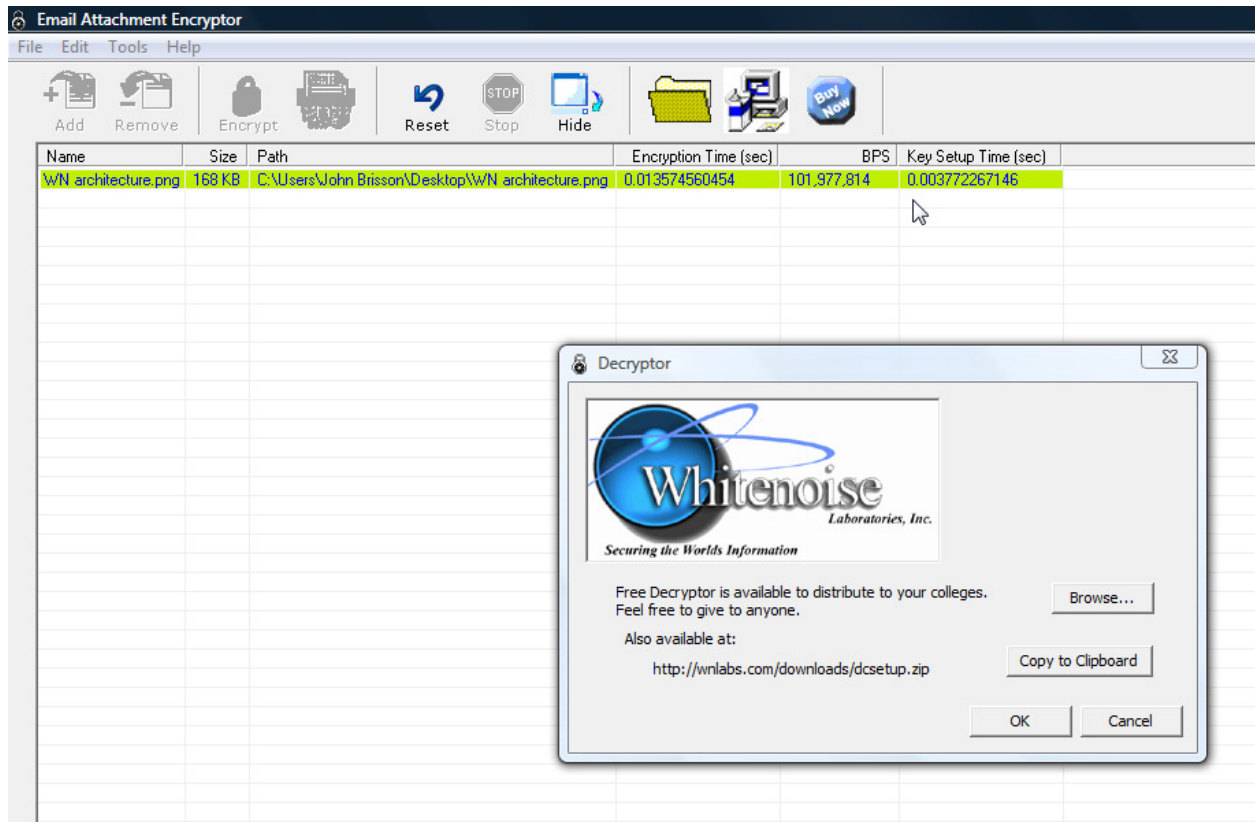


The Buy Now button is now deactivated. This application is completely free.

You are ready to go. Click the Add button and browse your computer to select the file that you want to safely send. Now click the Encrypt button and the following box comes up. Enter two pass phrases that you will remember and can tell your friend. Confirm your second pass phrase. Use the Browse button and have the encrypted file saved to you Desktop. Click Okay.



For the curious, the utility will give you extra information about the encryption process.



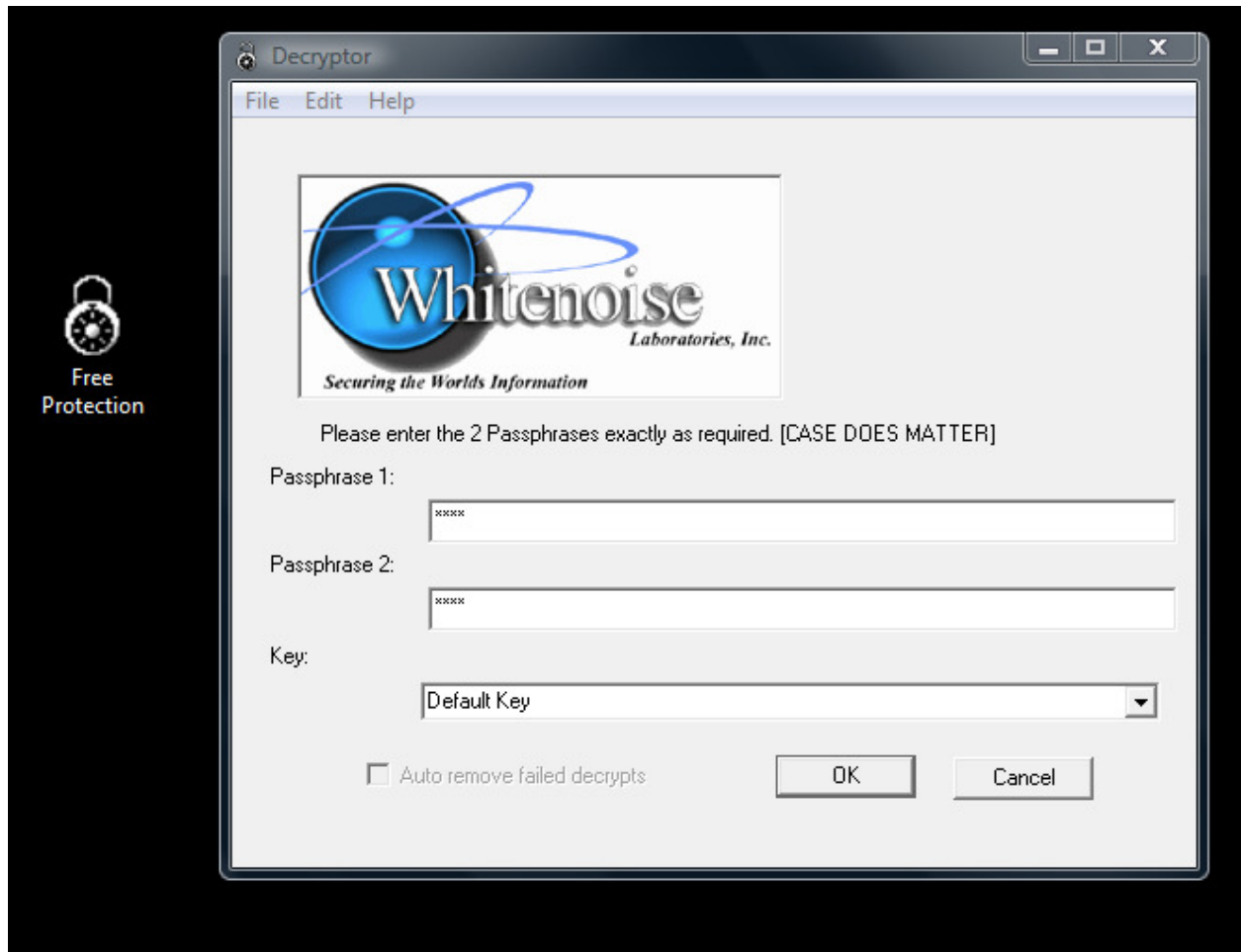
The button with the computer icon will let you copy the address where anyone can go and download the decrypting utility for free. This will be for first time uses who are receiving an encrypted file.

Go to your email application. Paste the decryptor link in the email. Write a cordial note to your friend. Attach the encrypted file and send it. That's it.

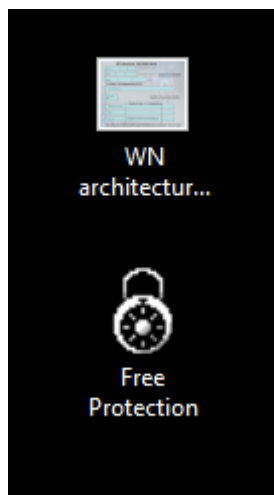
To decrypt a file click on the encrypted attachment.



Enter the two pass phrases chosen and click OK.



The file decrypts. That's it.



Enjoy simple privacy and peace of mind. *Whitenoise Labs team*

## Learn more about Whitenoise

One single key distributed one time will provide ALL network security and prevent all known attacks.

Whitenoise Technologies is really about complete network and communications security. One exponential key creates an infinite number of one-time-pads. One protocol, Dynamic Identity Verification and Authentication DIVA performs ALL network security functions including perfect identity, secure network access, continuous dynamic authentication, authorization, signature, non-repudiation, inherent intrusion detection and automatic revocation without human intervention.

It all starts with being able to create a key streams of exponential length and storing them in a tiny space. For example only about 150 bytes of information is required to store or transmit and still be able to create a key stream quadrillions of bytes long. Then Whitenoise just manages indexes into these key streams without ever having to transmit either key or offset information after the initial key provision.

Prove it to yourself – it takes moments and its fascination.

The key creation utility has been included in your zipped download.

1. Unzip WNsppedUtilitydemonstrator.zip
2. Go into the WNsppedTester folder.
3. Click Setup and follow directions.
4. Reboot computer.
5. Go to Start
6. Go to All Programs
7. Go to WN DLL
8. Click New Whitenoise Encryption

Note two things:

Key technologies are generally tested and measured when they are used for encryption. Remember one Whitenoise key does ALL network security functions.

Whitenoise technologies are NOT mutually exclusive with PKI. We run alongside and fix their fatal flaws.

## Let's make a key

Maximize the screen for better visibility.

Click File and then click Create Key.

A Whitenoise key is constructed of a variable number of subkeys of prime number length.

Using the pull down menu for Key 1 Length and choose a value. As you continue to choose values for each subsequent subkey you will see at the top bar that the Subkey Length "SK len =" value is exponentially increasing. The length of a Whitenoise key stream is determined by multiplying the subkey lengths in bytes together.

In the example below we created a colossal key of greater than 35 hextrillion bytes long and we only need to store or transmit 1960 bytes of key structure information to exactly recreate this key stream. And, we can use it faster than 128 bit keys.

Give your Key and Key File Name one that you will remember.

Click OK.

Key Length	Value
Key 1 Length	43
Key 2 Length	179
Key 3 Length	229
Key 4 Length	227
Key 5 Length	233
Key 6 Length	241
Key 7 Length	251
Key 8 Length	191
Key 9 Length	193
Key 10 Length	173

Key Name: colossal key      Key File Name: colossal key

Key Number: 1

Buttons: Ok, Cancel

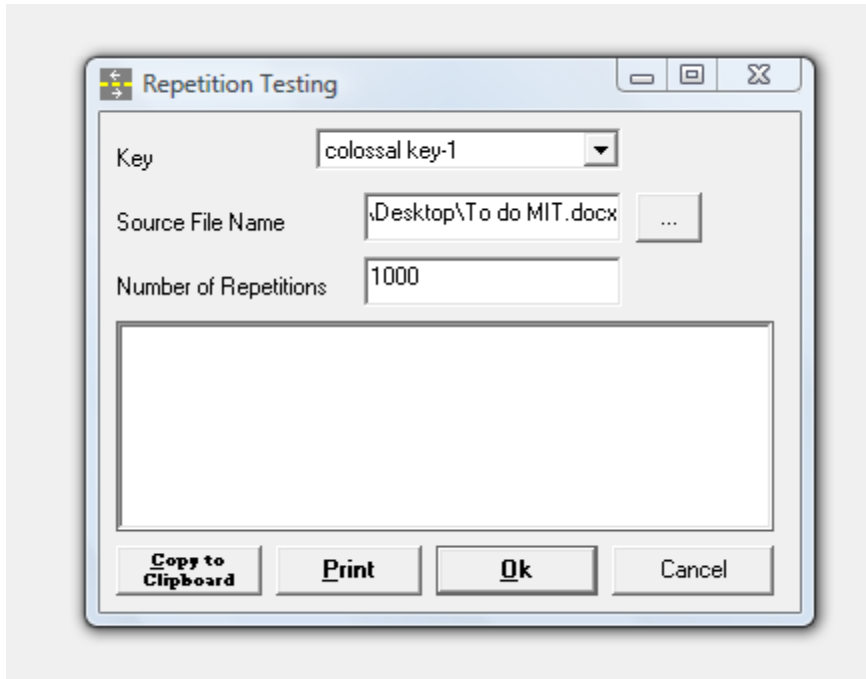
## Let's test this key

Go to File and choose repetition tester. This is based on standard AES key testing utilities.

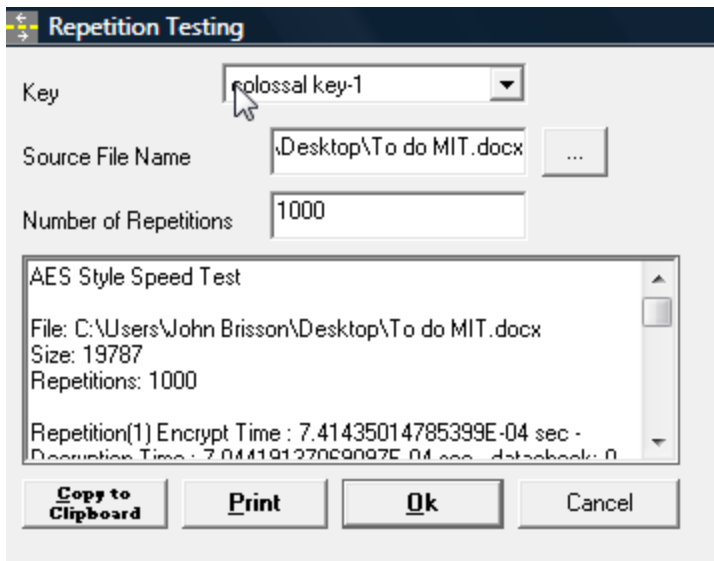
Using the pull down menu, choose the key you just created.

Using the browse button grab a sample file to test. For these purposes a text file about 1 Mg will be suitable. This will be the Source File that we are going to encrypt and decrypt.

Choose about 1000 for the number of repetitions. Click OK.

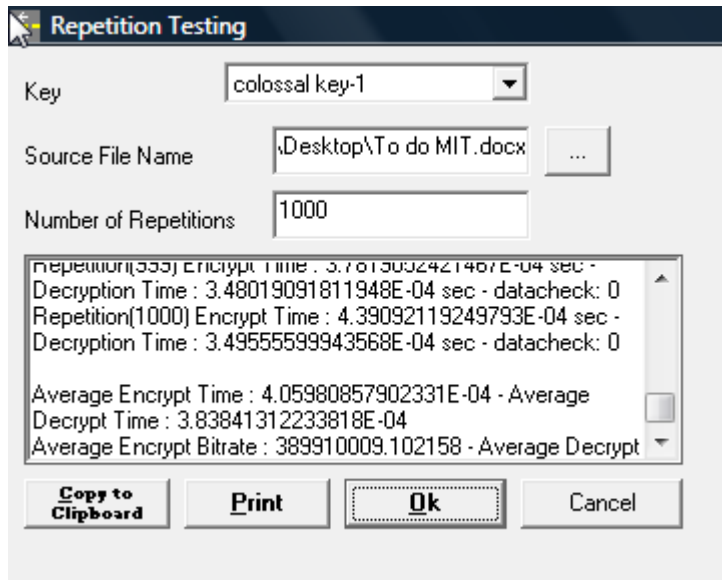


Whitenoise rapidly encrypts and decrypts this file. In this example, below, you can see that we chose a file of 19,787 bytes and encrypted and decrypted it 1000 times.



Scrolling to the very bottom, in the picture below you can see Repetition (1000). You can see the average encryption time was .0004 seconds. You can see the average decryption time was .0003 seconds. You can see the average encryption rate was 389,910,009 bits per second.





Because the key streams are so large and deterministic they will easily outlast the life of any person or device.

Static portions of the key stream can be used for specific accounts, functions, or things we need in every day life like passport numbers, credit card numbers, health care numbers etc.

The balance of the key stream is used as a one-time-pad for unbreakable security.

Please visit [www.wnlab.com](http://www.wnlab.com) and go to the Technology pull down menu. Choose YouTube videos to see narrated demonstrations and presentations to learn about the future of security including how Whitenoise keys are constructed, factoring Public keys, how DIVA works etc.

*Thank you from the Whitenoise Team*