Subject: Setting up the random number service
Posted by David_T on Tue, 23 Nov 2010 17:14:17 GMT
View Forum Message <> Reply to Message

The random number service is not up -- we plan to include it later!

Subject: Re: Setting up the random number service
Posted by David_T on Fri, 26 Nov 2010 06:18:34 GMT
View Forum Message <> Reply to Message

We have some positive news, the random number server has been tested. We need some download pages for the random numbers. We plan to include source code and Windows EXE so you can download random numbers from our server. :o

http://www.randomserver.dyndns.org/client/random.php

Subject: Re: Setting up the random number service
Posted by David_T on Sun, 28 Nov 2010 11:42:37 GMT
View Forum Message <> Reply to Message

the format of the test page is random bytes, so we have a flat distribution in the range [0..255].

Subject: Re: Setting up the random number service
Posted by randomserver on Sat, 01 Jan 2011 21:32:47 GMT
View Forum Message <> Reply to Message

I have set up a new page for the random numbers where you can select different distributions

Subject: Re: Setting up the random number service
Posted by David_T on Sun, 02 Jan 2011 02:01:40 GMT
View Forum Message <> Reply to Message

Thank you! Much better than the test page ! :)

Subject: Re: Setting up the random number service
Posted by KeithW on Tue, 11 Jan 2011 04:47:19 GMT
View Forum Message <> Reply to Message

I have a question on the random number generator of the server. Can you describe how it works?

Subject: Re: Setting up the random number service
Posted by David_T on Fri, 14 Jan 2011 05:04:13 GMT
View Forum Message <> Reply to Message

The random numbers come from a hardware random number generator that is attached to the server. The random numbers are tested, and then there is a cryptographic processing. The processing take place in a small memory buffer. Excess random numbers are transferred to a disk buffer, where they are stored until a peak load occurs.
The numbers that you see on screen is taken from the random number application through a webb-api. This is available externally, so you can run the random number application on your own computer. The version we have here is available for download.

All numbers produced are true random numbers. This imply that the server can run out of random numbers. If that happens, the server will become unresponsive until the request can be fulfilled directly from the hardware.

Subject: Re: Setting up the random number service
Posted by EdwardCasey on Thu, 15 Dec 2011 10:40:02 GMT
View Forum Message <> Reply to Message

Can you post some information about non-deterministic random numbers.

Subject: Re: Setting up the random number service
Posted by KeithW on Thu, 15 Dec 2011 11:44:15 GMT
View Forum Message <> Reply to Message

Try Math and Practical

Subject: Re: Setting up the random number service
Posted by TRNG98 on Tue, 03 Jan 2012 12:04:39 GMT
View Forum Message <> Reply to Message

Information on the properties of unbiased random numbers can be obtained by studying tests for random number generators.
The properties of circuits should follow good engineering practice, as well as security requirements. You may learn about security requirements from certification institutes.

I have also seen many esoteric machineries to produce random numbers. Many of these are not suited for industry use.

Subject: Re: Setting up the random number service
Posted by TRNG98 on Sat, 14 Jan 2012 08:27:40 GMT
View Forum Message <> Reply to Message

I have a new version where you can download random numbers to a file.
I have seen a discussion about the random alphabet; I make an update on that too.

New version coming soon :flower: :flower:

Subject: Re: Setting up the random number service
Posted by randomserver on Mon, 16 Jan 2012 01:44:43 GMT
View Forum Message <> Reply to Message

:welcome:
the test file is random_12.php

Subject: Re: Setting up the random number service
Posted by David_T on Wed, 18 Jan 2012 08:17:48 GMT
View Forum Message <> Reply to Message

If you are currently testing the new download service, please kindly download only small files, as the server is currently running low on the buffer.
There are no restrictions as long as you intend to use the downloaded files for some purpose !
Thank you.

Subject: Re: Setting up the random number service
Posted by TRNG98 on Wed, 18 Jan 2012 09:14:17 GMT
View Forum Message <> Reply to Message

This is a preliminary introduction text to the free encryption download:

The Two Time Pad Encryption System

The manual encryption is intended to stimulate interest in encryption and computer security. In this implementation, where the encoding tables are sent over the internet, the level of security is limited. For professional use we recommend generating the tables on a local machine. The tables is intended to be printed on paper and used with a pen without any electronic aids. The typical use would be to send home a report with evaluation of a product or service.

In the classic one-time-pad, the plaintext letters are added to a key by addition. A typical implementation is to convert the plaintext into numerical form, and then encrypt the plaintext numbers by adding a secret numerical key. Instead, this implementation use random substitution alphabets as the key. To make decoding easier, the substitution is reciprocal, so if the letter A

encrypts to W, the letter W will encrypt back to an A. A substitution alphabet is much stronger compared to a simple addition of letters, so each alphabet can be used for several letters before there is a risk that the code can be broken.

In the one-time-pad the key may be used only once, hence its name. Preventing reuse of the key is typically a problem, and in practice it has been difficult to prevent this. In this table system, where each alphabet can encrypt not only a single letter, but a small number of letters, we can introduce protection also against accidental reuse of the tables by limiting the number of processed letters to half the calculated maximum. Since the tables can encrypt two messages, we call the system the Two Time Pad.
Of these two encryptions we normally use only one, and save the other if the wrong sheet is used, or generally as a protection for other mistakes.

The system consists of a group number, that is used when finding the proper decoding page for decryption. Then there is a set of lines where the plaintext characters shall be written. The plaintext row is marked with a "P" while the ciphertext row, below, is marked with a "C". There are five rows for each group of substitution tables.
Some character positions are blocked out with XXXX marks, these character positions shall be skipped over. This also limits the number of characters each alphabet encrypts to a maximum of four. Straight under the plaintext character is the alphabet, and the encryption is reciprocal, so the same alphabet (same sheet) can be used for decryption. This imply that the receiving station need merely a photocopy of the tables, and not a separate (different) decryption sheet.

To set up the system, adopt the provided character set to match your application. If you work in a double currency environment, assign two characters to label the corresponding currencies. If you work with many people, instead of naming these you can make a list where each employee is given a two or three letter code. If you
need to give an evaluation of things you work with, you can create a grade or ranking, so that a rough estimate of your opinion about a task or issue can be described simply by giving the corresponding grade or ranking code.

If you need to write down a phrase or name exactly, and you cannot do this due to character set limitations, you can include the IBM-PC numerical character code; on the PC you can enter a character by holding down ALT and then type a three digit code on
the numerical keypad. The result will be code-page or font dependent, so you need to agree on this in advance. For example "We are in Ã–stersund" will be "WE+ARE+IN+/153STERSUND", the ALT+153 produces the Ã– character on the PC.

Note that the digit 0 and letter O is identical and also digit 1 and letter I. They share the same encoding character. A space character between words can often simply be removed, but, to make decoding more easy, you can use one of the special characters as word separator such as + or @.

To set up the system for three nodes you print tables with group numbers 0-299 for the first node, groups 300-599 for second node and groups 600-899 for the third node. All nodes need a copy of all the tables. To send a message a node write the message using its own range of group numbers; this is to limit the possibility of reuse of the keys. Using the tables twice shall be avoided!

The language of the message shall be clear and to the point. Avoid writing polite phrases! Use words like NO, WRONG, IDIOT, FRAUD, FAKE, BROKEN, ABORT, STOP, OK, GO, SEND, and similar.

To print the tables on the web service, enter the first and last group numbers as the A and the B parameter. One group will be one page with substitution alphabets. To adjust the width of the printout to match your paper, the number of columns is entered as the N parameter. Use the maximum N that fit on the page. A number of 8-16 is recommended.

When the sheets has been used, they shall be destroyed immediately, so only the encrypted message remains. On the decoding side it is a good practice to slightly re-write the message so that the exact letters cannot be obtained, and then destroy the encryption sheets. Note that actually destroying the sheets is not an easy task, like in a hotel room, and can be rather problematic in some situations especially if you want to do it well.

Even if this system is intended only as an demonstration, remember that in some countries the concept of privacy is simply not understood and absolutely not respected. Government agencies, with the best and most modern equipment, will generally work with local companies and assist in any way they can. Note that cell phones or SMS messages will not be safe in such an environment. The encryption of cell phones is controlled by the local authorities, and provide no protection. It can most likely be broken easily using the right tools.

If you wish to set up the system, you should do so on a stand-alone computer that is not connected to the internet. You generate the tables using a TRNG98 true random number generator. The software is supplied with the product.

Subject: Re: Setting up the random number service
Posted by FreddoW on Tue, 24 Jan 2012 08:53:57 GMT
View Forum Message <> Reply to Message

Eh? THe random_12.php isn't there -- is the new software uploaded?

Subject: Re: Setting up the random number service
Posted by randomserver on Sat, 28 Jan 2012 05:46:07 GMT
View Forum Message <> Reply to Message

Yes, it has been uploaded.
All numbers produced comes directly from a true random number generator.

Subject: Re: Setting up the random number service
Posted by KeithW on Wed, 08 Feb 2012 12:59:37 GMT
View Forum Message <> Reply to Message

I think the crypto pages from the true random number generator is super.
8)

Subject: Re: Setting up the random number service
Posted by FreddoW on Thu, 22 Mar 2012 23:32:28 GMT
View Forum Message <> Reply to Message

Mi, 18 Januar 2012 10:14 schreib TRNG98:Even if this system is intended only as an demonstration, remember that in some countries the concept of privacy is simply not understood and absolutely not respected.
I don't really follow you thought. Can you give an example ?

Mi, 18 Januar 2012 10:14 schreib TRNG98:Note that actually destroying the sheets is not an easy task, like in a hotel room, and can be rather problematic in some situations especially if you want to do it well.
Again I don't see what the problem should be. Please explain!

Q1:
Do the reciprocal property of the alphabets weaken the encryption? Would it be possible to construct separate tables, and use general substitution tables?

Q2:
It it legal to communicate by encryption ?

Q3:
Any third party may take a copy of the tables while I download them from the net. Is it possible to download the tables in an encrypted form, or is there any other solution?

Looking forward towards your response.
Fred Williams

Subject: Re: Setting up the random number service
Posted by TRNG98 on Thu, 12 Apr 2012 14:58:45 GMT
View Forum Message <> Reply to Message

I was thinking about a country like China, where it might be completely legal to collect information and monitor the phone, and there simply are no cell phone security.
On the question of destruction of encryption sheets, incinerating these in the hotel room, mix the ashes, and discard the ashes; I was thinking about the hotel room smoke detector. You are normally not supposed to light a fire in your hotel room!

Q1:
Yes that will work, and the reciprocal alphabets is a drawback. Note that the trade-off is not on security, but rather on how many letters that can be encrypted on each alphabet while remain information-theory secure.
The reciprocal alphabets have I=LOG(48*46*44*...*4*2)/LOG(2)
Ordinary alphabets have I=LOG(48*47*46*...*4*3*2*1)/LOG(2)
The number of letters will be about n=I/(5.6-1.0)

Q2:
I have never heard of that secret communication would be illegal. If your government demand to eavesdrop on all that you say, scrap the government.

Q3:
Well, if you download 300 sheets right now, print them, and store them at a safe place, your local signal intelligence department shall have a gold star if they can produce a backup copy several months later when needed. After all, you may simply discard the download...
The best way is to buy a hardware random number generator, and print the sheets locally on a machine that is off-line.

Subject: Re: Setting up the random number service
Posted by KeithW on Mon, 16 Apr 2012 07:34:53 GMT
View Forum Message <> Reply to Message

The server statistics is now printed on the front page. I can see my IP when I download some numbers; the disk buffer could need some explanation.

Subject: Re: Setting up the random number service
Posted by David_T on Thu, 19 Apr 2012 14:32:29 GMT
View Forum Message <> Reply to Message

Yes; I have just uploaded an updated version.

Subject: Re: Setting up the random number service
Posted by FreddoW on Fri, 20 Apr 2012 07:24:35 GMT
View Forum Message <> Reply to Message

The display window for the server status don't work on Microsoft Explorer ...

Subject: Re: Setting up the random number service
Posted by TRNG98 on Fri, 20 Apr 2012 16:05:43 GMT
View Forum Message <> Reply to Message

Hi!
I have sent a new update, that reasonably go on Windows!

Subject: Re: Setting up the random number service
Posted by David_T on Fri, 20 Apr 2012 16:07:52 GMT
View Forum Message <> Reply to Message

I just updated the service.
The automatic update now also run on Microsoft Explorer.
:flower:
