The Manual One-time Pad

This page is a guideline to the use of **one-time pads** and how to set up one-time pad communications in only four steps. One-time pad encryption is unbreakable if properly applied. However, the security of the system entirely depends on the correct use of the one-time pads and the their secure distribution. To obtain the highest level of security it's an absolute must to strictly follow all rules without exception. These rules are not negotiable. One-time pad is not a practical encryption system. However, if properly used, it will be absolutely secure and unbreakable.

One-time Pad Communication in Four Steps

- **Step 1: Creating One-time Pads**
- **Step 2: Preparing the Message**
- **Step 3: Encryption and Decryption**
- **Step 4: Important Security Issues**
- **A Software Number Generator**
- **Summary**

Step 1 - Creating One-time Pads ▲

The basis of the system are the one-time pad pads. A one-time pad can be a single sheet, a booklet, a roll of paper tape or a paper strip that contains series of random numbers. These could be stored in tamper-proof sealed containers (plastic, metal or cardboard) to ensure that the series of numbers are used one by one and to prevent or at least detect unallowed disclosure of unused numbers.

The numbers must absolutely be truly random. To generate these random numbers, the most practical option is to purchase a hardware based generator with random noise source (PC card or USB device). Firms like **Mils Electronic** and **IDQ** offer hardware RND generators.

A second way is to generate the numbers purely with software. However, such generators should be selected with care. Software, simply based on the computer RND function, will not produce secure random numbers! At the bottom of this page you can download a **software number generator**. If you generate the random numbers on a computer, you must always use a stand-alone computer, never connected to a network. No single computer is secure if ever connected to a network!

Another very secure and truly random method - although time consuming - is to select the random numbers manually. You could use five ten-sided dice. With each throw, you have a new five-digit group (see image right). Such dice are available in toy stores or you could make them yourself (**dice template**).

Never ever simply use normal six-sided dice by adding the values of two dice. This method is statistically unsuitable to produce values from 0 to 9 and thus absolutely insecure (the total of 7 will occur about 6 times more often that the values 2 or 12). Instead, use one black and one white die and assign a value to each of the 36 combinations, taking in account the order/colour of the dice (see table below). This way, each combination has a .0277 probability (1 on 36). We can produce three series of values between 0 and 9. The remaining 6 combinations (with a black 6) are simply disregarded, which doesn't affect the probability of the other combinations.

```
B   W         B   W         B   W        B   W        B   W
1 + 1 = 0     2 + 1 = 6     3 + 1 = 2    4 + 1 = 8    5 + 1 = 4
1 + 2 = 1     2 + 2 = 7     3 + 2 = 3    4 + 2 = 9    5 + 2 = 5
1 + 3 = 2     2 + 3 = 8     3 + 3 = 4    4 + 3 = 0    5 + 3 = 6
1 + 4 = 3     2 + 4 = 9     3 + 4 = 5    4 + 4 = 1    5 + 4 = 7
1 + 5 = 4     2 + 5 = 0     3 + 5 = 6    4 + 5 = 2    5 + 5 = 8
1 + 6 = 5     2 + 6 = 1     3 + 6 = 7    4 + 6 = 3    5 + 6 = 9

              THROWS WITH BLACK 6 ARE DISCARDED
```

Another good source of randomness would be a lotto system with balls, numbered from 0 to 9. After extracting a number, that ball must be mixed again with the other balls before extracting the next number. More about generating random numbers on the **one-time pad page**.

A default one-time pad sheet usually contains 50 groups of 5 random digits, which is sufficient for one normal message, and each one-time pad sheet should have a unique first group of five digits. This first group will be used to identify the key and is not used in the encryption process. A one-time pad set consist of two identical one-time pads. To establish a one-way communication you will only need one OUT pad for the sender and one IN pad for the receiver. To communicate in both directions both sender and receiver need OUT and IN pads. Never use a single pad to communicate in both directions!

Example of an OUT booklet No 1234 and its sheet No 00015:

```


     ONE WAY
ENCRYPTION PAD

 C
C
 R            OUT
R
 Y
Y
 P          NR  1234
P
 T
T
 O
O



          S E C R E
T
```

```
                        00015

  74061 66599 83953
09280 65571
  63520 33281 77791
08682 03571
  50328 17473 91793
91901 59147
  17384 08557 35976
97056 60440
  09806 14445 48755
27860 37199
  97514 01656 05503
10236 71732
  44113 85092 60337
36566 36444
  30022 97942 25861
31606 34387
  04506 36113 14031
79425 46823
  39301 09391 85029
17535 68745

          DESTROY
AFTER USE
```

© D Rijmenants 2008

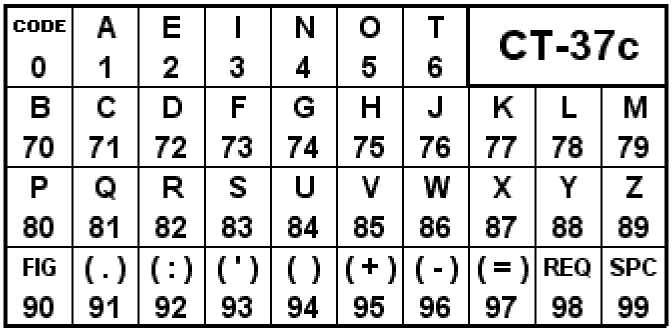
When used in clandestine circumstances, the most practical key pads for the person in the field are those that are printed on very small thin paper sheets (see photo). These are easy to hide and destroy. Never store them on a computer, memory stick or CD. These will always leave traces, even after they were erased, and total destruction is never guaranteed. There are several specialized techniques to retrieve computer data, but none to retrieve a burned or digested paper key pad. In critical situations, it's harder to quickly dispose or destruct a memory stick or floppy disk than to eat a small paper sheet.

Step 2 - Preparing the Message ▲

Before we can encrypt a message with a one-time pad, we need to convert it into numbers. This conversion is not a type of encryption and offers absolutely no protection whatsoever! The conversion only prepares the plain text for the actual encryption process. In our example, we use the CT-37c conversion table. You can find other variations of the checkerboard conversion table **on this page**.

The CT-37c table is an extended straddling checkerboard. The table is easy to remember by its most frequent English letters "AEINOT" in the top row, preceded by the "CODE" (0) field. The following two rows contain the remaining letters. The fourth row contains "FIG" (90), the punctuations (less critical to memorize) and the "REQ" (98) and "SPACE" (99) fields.

The Conversion Table



CODE 0	A 1	E 2	I 3	N 4	O 5	T 6	CT-37c		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	S 83	U 84	V 85	W 86	X 87	Y 88	Z 89
FIG 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	SPC 99

Another way to represent the table

```
           ENCODE
DECODE

 A-1   K-77  U-84    (.)-91
0-CODE 70-B  80-P  90-FIG
 B-70  L-78  V-85    (:)-92
1-A    71-C  81-Q  91-(.)
 C-71  M-79  W-86    (')-93
2-E    72-D  82-R  92-(:)
 D-72  N-4   X-87    ( )-94
3-I    73-F  83-S  93-(')
 E-2   O-5   Y-88    (+)-95
4-N    74-G  84-U  94-( )
 F-73  P-80  Z-89    (-)-96
5-O    75-H  85-V  95-(+)
 G-74  Q-81  FIG-90  (=)-97
6-T    76-J  86-W  96-(-)
 H-75  R-82  SPC-99
77-K  87-X  97-(=)
 I-3   S-83  CODE-0
78-L  88-Y  98-REQ
 J-76  T-6   REQ-98
79-M  89-Z  99-SPC
```

Using the CT37c table is easy. All characters are converted into their one-digit or two-digit value. To convert numbers, always use "FIG" before and after one ore more digits. Each digit is written out three times to exclude errors. You can use spaces and punctuations within the "FIG" mode. An example: "1.5 KG" = "90 111 91 555 90 77 74". The "REQ" or "REQUEST" field enables questions and spaces are created with the "SPC" field. The apostrophe (93) can be used as both apostrophe and comma. The "CODE" field is the codebook prefix and is used before each codebook value. The use of spaces before and after codebook words is not necessary.

The use of a codebook is optional. However, a codebook can reduce the length of the ciphertext and transmission time enormously. One can always omit the codes if the receiver has no copy of the codebook. The codebook can contain all kinds of words and/or small phrases about message handling and technical, tactical, logistic or medical expressions. The codebook should contain the most often used words and expressions that would normally be converted with the default table into more than four digits. Since one-time pad encryption is applied, it is not necessary to have a random codebook numbering or to keep the codebook secret. A codebook system does not always require a large book with thousands of expressions. Even a single codebook sheet with carefully selected expressions, as shown below, can contain enough practical information to reduce the message length enormously.

000	ABORT	253	DECODE	505	MILITARY	758	STREET
019	ACCEPT	262	DELAY	514	MONEY	767	SUBWAY
028	ACCESS	271	DIFFICULT	523	MONTH	776	SUCCESS
037	ADDRESS	280	DOCUMENT	532	MORNING	785	SUPPLY
046	AFFIRMATIVE	299	ENCODE	541	MORSE	794	SUPPORT
055	AGENT	307	EVENING	550	NEGATIVE	802	TELEPHONE
064	AIRPLANE	316	EXECUTE	569	NIGHT	811	TODAY
073	AIRPORT	325	FACTORY	578	OBSERVATION	820	TOMORROW
082	ANSWER	334	FAILED	587	PASSPORT	839	TRAIN
091	AUTHORITY	343	FERRY	596	PERSON	848	TRANSFER
109	BETWEEN	352	FLIGHT	604	PHOTOGRAPH	857	TRANSMIT
118	BORDER	361	FREQUENCY	613	POSITIVE	866	TRAVEL
127	BUILDING	370	HARBOUR	622	POSSIBLE	875	TRUCK
136	CANCEL	389	HELICOPTER	631	POWER	884	UNABLE TO
145	CHANGE	398	HIGHWAY	640	PRIORITY	893	URGENT
154	CIVILIAN	406	IDENTITY	659	PROBLEM	901	VERIFY
163	COMPROMISE	415	IMMEDIATE	668	QUESTION	910	WEEK
172	COMPUTER	424	IMPOSSIBLE	677	RADIO	929	WITHIN
181	CONFIRM	433	INFORMATION	686	RECEIVE	938	YESTERDAY
190	CONTACT	442	INSTRUCTIONS	695	RENDEZVOUS	947	DISREGARD MSG FROM
208	COORDINATE	451	LOCATE	703	REPEAT	956	DO NOT ANSWER
217	COUNTRY	460	LOCATION	712	RESERVATION	965	FORWARD THIS MSG TO
226	COVERT	479	MAIL	721	ROUTINE	974	REPEAT YOUR MSG FROM
235	CURRENT	488	MEETING	730	SATELLITE	983	READABILITY (1 TO 5/5)
244	DANGER	497	MESSAGE	749	SHIP	992	SIGNAL STRENGTH (1 TO 5/5)

Some words in the codebook are extendable or changed by addition of one or more characters. with the CT-37 conversion table from above, the plural of 0596 (PERSON) will be 059683 (PERSONS). The past perfect of 0686 (RECEIVE) will be 068672 (RECEIVED), and 0901 (VERIFY) will be 090172 (VERIFYD or verified). Words can also get another meaning. 0686 (RECEIVE) becomes 068682 (RECEIVER), 0857 (TRANSMIT) becomes 085782 (TRANSMITR or transmitter) and 0226 (COVERT) becomes 02267888 (COVERTLY). The FIG code can be omitted when a figure is expected. Thus, SIGNAL STRENGHT 4 can be written as 0992444.

In our example we will also use the codebook from above. Note the strange non-consecutive values in the codebook. These values are carefully selected and will always enable the detection of single-digit errors and in most cases also two-digit errors. An error will always result in a non existing code. Simply using the values 00 trough 99 for our 100 codebook words is not recommended, as a single-digit error would result in a completely wrong word! Of course, the codebook can be adapted for any specific use.

Let us convert the text "MEETING BERLIN CANCELLED. TRAVEL 25 JAN TO ZURICH WITH NEW PASSPORT."

```
 MEETING B  E R  L  I N  CANCEL-D  .  TRAVEL    2   5      J  A N
 0488    70 2 82 78 3 4  0136   72 91 0866   90 222 555 90 76 1 4 99

 T O    Z  U  R  I C  H     W  I T H     N E W  PASSPORT.
 6 5 99 89 84 82 3 71 75 99 86 3 6 75 99 4 2 86 0587    91


 In groups:
 04887 02827 83401 36729 10866 90222 55590 76149 96599 89848 23717 59986
36759 94286 05879 19191
```

The final group should always be completed with full stops (919....). Note that, with the help of our little code sheet, the 68 characters of the message (spaces and punctuations included) are converted into no more than 80 digits! This gives a very good 1.17 digit/letter ratio. Of course, one could also omit all spaces where readability is maintained and use various abbreviations like "YR" for "YOUR", "WTH" for "WITH" or "RTRN" for "RETURN". This would reduce the message length even more.

Step 3 - Encryption and Decryption ▲

Once our message is converted into digits we can start the encryption. First, we tell the receiver which key was used. This is done by adding the first five-digit group of the one-time pad sheet at the beginning of the message. This first group of the one-time pad should never be used in the encryption process. Always start enciphering from the second group of the pad. This method of identification doesn't reveal any order of the messages, nor how many messages were actually sent. In the example we skip the identification group 74061 of the pad.

Write down the plaintext digits from Step 2 in groups of five, write the numbers, obtained from the one-time pad key, underneath the plaintext and subtract the one-time pad key from the plaintext, digit by digit and from left to right. Subtraction is performed without borrowing (e.g. 5 - 9 = 15 - 9 = 6). Always complete the last group of plaintext with zeros. In the example we used the one-time pad sheet No 00015 from booklet 1234 as shown in Step 1.

```
 Plain  : KEYID 04887 02827 83401 36729 10866 90222 55590 76149 96599 89848
23717 59986 36759 94286 05879 19191
 OTP (-): 74061 66599 83953 09280 65571 63520 33281 72791 08682 03571 50328
17473 91793 58402 00658 45973 85273
          --------------------------------------------------------------------
---------------------------------
 Result : 74061 48398 29974 84221 71258 57346 67041 83809 78567 93028 39520
16344 68293 88357 94638 60906 34928
```

Always destroy the key sheet immediately after finishing the encryption, even if it still has unused groups. A new message should always be encrypted with a new sheet. NEVER reuse a pad!

Below the complete message, with the key identification number 74061 as first group. If the message is sent by radio, in voice or Morse, it is recommended to relay all groups twice to exclude errors (f.i. 74061 74061 48398 48398 and so on). If the receiver's callsign is "306", the message could look like this:

```
306 306 306

74061 48398 29974 84221 71258
57346 67041 83809 78567 93028
39520 16344 68293 88357 94638
60906 34928
```

To decrypt the message, the receiver verifies the first group of the message to ensure that he uses the correct one-time pad sheet. Next, he writes the proper one-time pad digits underneath the ciphertext and adds the key to the ciphertext, digit by digit, without carry (e.g. 9 + 6 = 5 and not 15). The first group is skipped as it is only used to identify the key.

```
 Ciphertext: 74061 48398 29974 84221 71258 57346 67041 83809 78567 93028
39520 16344 68293 88357 94638 60906 34928
 OTP Key(+): 74061 66599 83953 09280 65571 63520 33281 72791 08682 03571
50328 17473 91793 58402 00658 45973 85273
             ----------------------------------------------------------------
-------------------------------------
 Plain text: KEYID 04887 02827 83401 36729 10866 90222 55590 76149 96599
89848 23717 59986 36759 94286 05879 19191
```

Finally, the receiver re-converts the numbers into plaintext letters with the help of his conversion table. One-digit and two-digit characters are easily distinguished: if the next digit is 1 to 6, you have a one-digit characters. If the next digit is 7, 8 or 9 you have a two-digit character and there's one more digit that follows. If the next digit is 0, a three-digit code follows.

Always use subtraction to encrypt and addition to decrypt.

Remember! Never keep a key sheet after it has been used to decrypt a message. This will compromise the key and the message! Destroy the key sheet immediately after use.

Step 4 - Important Security Issues ▲

This section contains important rules that should be followed when using one-time pad encryption and communications. These rules are not negotiable. Virtually all one-time pad communications that were compromised at some point, violated one or more of these rules. Even a small and seemingly insignificant error can result in unauthorized decryption of the messages. Insecure communications enable the eavesdroppers to link the messages to the sender or receiver who wanted to stay anonymous. Often, the users were thoroughly instructed beforehand on how to do things but believed that those little details didn't matter. They were wrong. It helps to be paranoia. However, if used properly, one-time pad is unbreakable. And yes, also unbreakable for the NSA, GCHQ or FAPSI. Read carefully!

- **The One-time Pads**

One-time pad encryption is only possible if both sender and receiver are in possession of the same key. Therefore, the keys must be exchanged beforehand by both parties. This means that the secure communications are expected and planned within a specific time frame. Enough key material must be available for all required communications until a new exchange of keys is possible. Depending on the situation, a large volume of keys could be required for a short time period, or little key material could be sufficient for a very long time period, up to several years.

Never store one-time pads on a computer, memory stick or CD. Erasing these media is very problematic and total destruction of used one-time pads, stored on these carriers, is never guaranteed. Specialized techniques exist to retrieve computer data, even after the data was deleted, and even after it was actually overwritten. The key must always be distributed physically, personally or by a trusted courier. Never send one-time pads electronically. Encrypting a one-time pad before sending it electronically, for instance with AES or some other strong algorithm, is useless and dangerous because it will lower its security from unbreakable down to the security of the used encryption.

The most important part of one-time pad is a secure key management. If the key isn't compromised, the message is mathematically unbreakable. It is clear that those who are responsible for creating and handling one-time pads should be subjected to the highest level of security screening. The number of persons who are responsible for generating the key material should be limited to an absolute minimum. As soon as a one time pad key pair is created, it must be numbered and registered. There should be a centralised (star topology) registration and distribution in order to know who has which keys where and when. If a key pad is used, outdated, revoked or compromised, the distributor or user must immediately inform the other parties and remaining copies of that key should be destroyed immediately. Never use a one-time pad more than once! If you do so, simple analysis will break all messages, encrypted with the reused one-time pad (see **one-time pad page**)!

A one-time pad is always compromised in the following cases:

- The pad is used more than once
- The pad was - even temporarily - not under custody of authorised personnel or securely stored
- A distributor or user is suspected to have violated security rules
- The pad has been exposed intentionally or by accident to other people
- The pad is lost or there is no proof of destruction
- If there's any doubt about the current or past situation of the pad
- Finally, if you don't know whether a one-time pad is compromised or not, it is compromised.

Never use a compromised one-time pad and always notify all users of compromised pads to destory those pads immediately!

- **Secure Encryption and Decryption**

Never ever use a computer to type a plain message or to encrypt or decrypt a message. This will always leave traces on the computer, even after being deleted. There's no such thing as a safe computer! Instead, write the message, the key and do the calculations on a single piece of paper on a hard surface, and destroy that paper after you finished encrypting or decrypting. The most convenient method is to burn the paper. It sounds paranoia but has its reasons! Check you encryption before sending the message. A single error could make the message unreadable or result in critical mistakes during deciphering. Once a message is encrypted, you can store it anywhere you like. It will stay unbreakable. However, for reasons of deniability, it's not recommended to store enciphered messages on a computer or any other easily accessible medium.

- **Ways To Communicate**

If interception of the communications and exposure of the identity and location of the sender/receiver doesn't endanger their privacy or personal security, physically, legally or otherwise, we can send the message by any means, even insecure. It's unbreakable anyway. This is the easy way. However, if identification of the involved persons, or the fact that they use encryption, endangers their privacy or personal security, they must communicate covertly or disguise their message.

Covert communications are a most difficult issue. Telephone, mobile or satellite phone, voice or text message, paper mail, e-mail and other Internet based communications are always to be considered completely unsafe. They enable identification of both sender and receiver. They should never be used to communicate covertly. Publicly available systems are a way to communicate anonymously. Some examples are a computer in a cyber café or library (of course without need for registration) or a public phone (with anonymously bought pre-paid card). A message can be posted or read from a cyber-café computer onto an Internet forum or any random on-line guestbook. However, it should never be possible to link time and place to the person that uses the public system. Although one might be using a publicly available system anonymously, it remains possible to retrieve time and location of the communication. In such case, a witness or security camera could link a particular time and place to the person who used that public phone or computer. Today, all electronic communications are stored for long periods, ready to be exploited if required. A phone call or mobile phone's text message is never a moment in time. It is a digital event that permanently resides in databases.

It should also be impossible to link a particular device to an intercepted communication. A mobile phone or a pre-paid card will link that particular phone or card to the communications. Once this link is found, it’s easy to link that message to other related messages. On-line e-mail accounts are also easy to link to a particular message and location. Using a mobile phone, pre-paid card or e-mail account, even one single time, will always leave traces and compromise that method of communicating, making it impossible to use that particular phone, pre-paid card or e-mail account for any other purpose in the future.

Shortwave radio is an ideal way to covertly receive messages over large distances. There's no way to detect the location of someone who receives radio signals. Having a simple household shortwave radio isn’t suspicious (of course, the frequency to receive the messages should never be stored in the radio memory). Sending a message covertly with a radio transmitter poses more risks. A broadcast can be located within seconds if the opponent has the proper direction finding equipment. The current SDR technology (Software Defined Radio) easily permits surveillance and interception of many signals simultaneous on several wide frequency ranges. The use of burst-transmission (transmitting very rapidly) might not be sufficient to avoid detection. Therefore, a radio broadcast is only suitable when the transmitter is located far away and out of reach of the opponent. Another possibility is to use special equipment that operates on unusual frequencies or uses a special type of electromagnetic or optical carrier. As you can read, it's very difficult to communicate truly anonymously in today's high-tech and fully digitized world without leaving any trace.

If the communications are not intended to relay a message over a large distances, but solely to deny any relationship between sender and receiver, a dead-drop or brush-pass can be used. A dead drop is a location that is used to secretly pass items or messages between two people, without requiring them to meet. The sender hides the message on a secret but publicly available location and gives a signal somewhere else (f.i. a chalk mark on a wall or chewing gum on a pole) to tell the receiver that a dead drop was delivered. The receiver empties the dead drop at any suitable moment. Both persons must agree upon a location for the dead drop and a type of signal and its location beforehand. Detection of a dead drop would require intensive surveillance of both sender, receiver and the dead drop location. A brush-pass is an encounter between sender and receiver on a pre-determined location where they quickly and surreptitiously exchange a message. This could be done by leaving the message inside a newspaper to be picked up immediately after by the receiver, swapping identical bags, or any unsuspicious action in a public place. A brush-pass is easier to detect during surveillance and poses more risks than a dead drop. One could always deny that a message was transferred but cannot deny there was a meeting with the other person.

- **Deniability and Steganography**

As you can see, it is all but easy to communicate securely. Another way to convey the message is to do this openly, but to disguise the message in such way that an eavesdropper won’t know that the message was sent. This technique is also called steganography (lit. hidden writing). There are various ways to insert or hide ciphertext numbers in a seemingly innocent letter or e-mail. Of course, the numbers in the text should always look unsuspicious. Simply inserting strange sequences of digits or some illogical values could draw suspicion. Also, simply converting the message into digits without encryption and then hide them in a message (a basic null cipher) is a completely insecure method and should never be used. Always encrypt your message before hiding it!

One method to hide the ciphertext digits in text is to assign a set of words to each digit and use these words to compose a readable and innocent looking text. If properly applied, the encrypted communications are fully deniable. To ensure flexibility and variations in the composed text, each digit should be represented by as many as possible words. You can see an example of a digit-to-words table **in this text file** (right-click and select "Save As" to download). You can select any of the 22 words that are assigned to a particular digit. To retrieve the digits that are hidden in the text, the table also contains a word-to-digit part in alphabetic order, to quickly find the digit that corresponds to a given word in the text.

In the following example, we hide the groups 74061 48398 29974, an enciphered fragment from "Meeting Berlin cancelled..." from above. We use our example **digit-to-words table** to find the words that we can use in our text. You may also use the plural of some the words (MOVIES, CARS, HOUSES...) as long as the word stays unchanged (to avoid confusion). Occasionally, but not too often, you can use ciphertext digits directly in your text wherever this looks unsuspicious ("It took me 40 minutes to..."). Now, here's an example of how to hide the three ciphertext groups with our digit-to-words table:

"I just got back from the office. I could use a holiday! A pool with some beer would do just fine. A bit more cash on my account would be usefull to pay my airplane. I wish I could leave for a whole month. By the way, read any good books or magazines lately? I always read whilst listening to the radio,with a good glass of wine in my lazy couch. Much better than watching football. I know, you cultural barbarian prefer a cigar and a newspaper."

Isn't that a nice and innocent looking piece of text (of course, in real life, you don't underline the words). Make sure to compose a text that makes sense. Writing about a trip you never made or about a family member or your dog that doesn't exist could blow your cover! Writing about things that you would like to have or to do, or about things in the future is pretty safe because such information is harder to verify by an eavesdropper. Make sure not to use any of the table words unintentionally, as this would add a wrong digit and makes the text undecipherable. Double-check your work!

The receiver checks each noun in his word-to-digit table to see if it relates to a digit. He writes down the extracted digits and deciphers the ciphertext message with the proper one-time pad. Although it will take quite a few sentences to hide a large message, this method provides good flexibility. Of course, you should compose your own table with frequently used words, maybe also with words related to your enviroment, and keep this table secret. A compromised digit-to-words table could affect your chances to fully deny the existens of a message in the text. Nevertheless, the message will stay unbreakable when the one-time pad, used to encipher the message, is kept secret or has been properly destroyed .

With this method, the hidden message is fully deniable because there is absolutely no way to detect or to prove its existence in the innocent looking text without the proper one-time pad key. Given the fact that in today's digital world virtually all means to communicate are prone to eavesdropping, this method is the perfect solution to send messages by postal mail, e-mail, on-line accounts, Internet forums and such. This is especially interesting in countries where the use of encryption is forbidden and ciphertext groups could get you in trouble. The communicating itself however will still be detectable (traffic analysis!). You only need a bit of literary fantasy and an excuse why you wrote each other. Note that this technique, but in combination with other encryption algorithms than one-time pad, could enable the eavesdropper to cryptanalyse and decipher the text! Only one-time pad offers cryptanalysis-resistant text and truly plausible deniability.

A second method to hide digits in text is by converting digits into letters with the help of a much smaller table. Unfortunately, this method is less flexible to compose the text. We use the 20 most frequent letters in the English language, divided in two groups: "ETAOINSHRD LCUMWFGYPB". Each digit from 0 to 9 is assigned to one from the 10 higher frequent letters (first group) and to one from the 10 lower frequent letters (second group). Next, we compose a text where every other word starts with one of the two letters that correspond to the given ciphertext digit. Of course, you can adapt the conversion table to the letter frequencies of any other language (see **letter frequencies** on Wikipedia, click column header icons to sort your language)

Below the table with digit-to-letter and letter-to-digit conversion. The distribution of letters is optimized for the English language to provide sufficient flexibility in devising words. Scrambling the order of the letters isn't necessary because we use one-time pad.

```
English optimized table

0 = E or L     A = 2  M = 3
1 = T or C     B = 9  N = 5
2 = A or U     C = 1  O = 3
3 = O or M     D = 9  P = 8
4 = I or W     E = 0  R = 8
5 = N or F     F = 5  S = 6
6 = S or G     G = 6  T = 1
7 = H or Y     H = 7  U = 2
8 = R or P     I = 4  W = 4
9 = D or B     L = 0  Y = 7

Unused letters: J K Q V X
```

In the following example, we again use the groups 74061 48398 29974. When converted into letter pairs, according to the table above, we have the following sequence of 15 letter pairs:

```
HY IW EL SG TC IW RP OM DB RP TC DB DB HY IW
```

You are free to choose either the first or second letter of each pair as first letter of every second word. An example of how such a text could look like this:

"I hope everything is OK. Last week seemed quite chaotic, no? I think relaxation would offer you definitely better results to calm down. Don't skip breakfast and handle your workload!

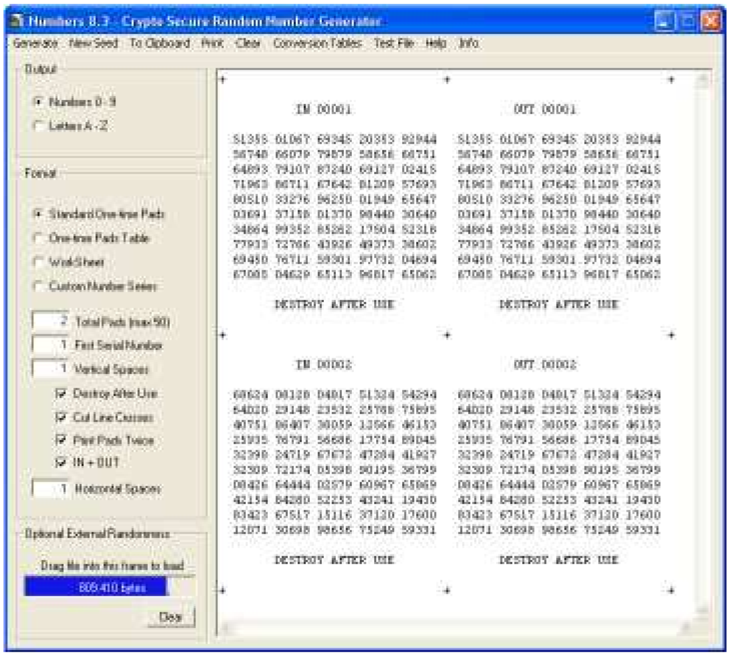
You can agree on starting off with either the first or the second word. If required, you can use one of the empty letters "JKQVX" instead of the 20 most frequent letters. In that case, the letter is simply discarded during deciphering and we continue with the next second letter. It gives you a bit more freedom to play with the text.

- **Personal Security and the Law**

Finally, there's also the issue of personal security. In some countries, it's forbidden by law to use this type of encryption. The reason is simple: some governments don't understand the word "privacy" and read their citizens' communications. One-time pads prevents them from doing so. That's why, in some countries, being caught with one-time pads or being identified as a person who used encryption could cost you more than money or freedom. One-time pads can cause serious health problems, and that's not a joke!

Numbers 8.0 Random number generator ▲

On this website you can **download Numbers 8.3**. With this Crypto Secure Pseudo Random Number Generator (CSPRNG) you can generate and print series of random numbers or letters, formatted as standard one-time pads, worksheets or custom series. You can also view and print different letter-to-digit conversion tables for use in one-time pad encryption. Although using a CSPRNG theoretically never achieves Shannon's perfect secrecy, it will be useful in practice to generate one-time pads. The huge size and the limited use of a given random seed, the astronomical number of possible generator states, the whitening by combining 14 generators, and the irregular partial use of the output make it infeasible to retrieve or predict the generated output. External randomness can be loaded into the software. The Numbers software is therefore a good software alternative to generate one-time pads.


Numbers 8.3 - Crypto Secure Random Number Generator
Generate
New Seed
To Clipboard
Print
Clear
Conversion Tables
Text File
Help
Info
Output
Format
Optional External Randomness
Drag file into this frame to load
Clear

Output
● Numbers 0 - 9
○ Letters A - Z

Format
● Standard One-time Pads
○ One-time Pads Table
○ WorkSheet
○ Custom Number Series

2 Total Pads (max 50)
1 First Serial Number
1 Vertical Spaces
☑ Destroy After Use
☑ Cut Line Crosses
☑ Print Pads Twice
☑ IN + OUT
1 Horizontal Spaces

809 410 bytes

```
+                                   +                                   +

            IN 00001                            OUT 00001

   51355 01067 69345 20353 92944       51355 01067 69345 20353 92944
   56740 66079 79879 58656 60751       56740 66079 79879 58656 60751
   64893 79107 87240 69127 02415       64893 79107 87240 69127 02415
   71963 86711 67642 81209 57693       71963 86711 67642 81209 57693
   80510 33276 96250 01949 65647       80510 33276 96250 01949 65647
   03691 37158 01370 98440 30640       03691 37158 01370 98440 30640
   34864 99352 85262 17504 52318       34864 99352 85262 17504 52318
   77933 72766 43926 49373 38602       77933 72766 43926 49373 38602
   69450 76711 59301 97732 04694       69450 76711 59301 97732 04694
   67005 04629 65113 96817 65062       67005 04629 65113 96817 65062

         DESTROY AFTER USE                   DESTROY AFTER USE

+                                   +                                   +

            IN 00002                            OUT 00002

   68624 08128 04017 51324 54294       68624 08128 04017 51324 54294
   64020 29148 23532 25788 75895       64020 29148 23532 25788 75895
   40751 86407 30059 12566 46153       40751 86407 30059 12566 46153
   25935 76791 56686 17754 89045       25935 76791 56686 17754 89045
   32398 24719 67672 47284 41927       32398 24719 67672 47284 41927
   32309 72174 05398 90195 36799       32309 72174 05398 90195 36799
   08426 64444 02579 60967 65869       08426 64444 02579 60967 65869
   42154 84280 52253 43241 19430       42154 84280 52253 43241 19430
   83423 67517 15116 37120 17600       83423 67517 15116 37120 17600
   12071 30698 98656 75249 59331       12071 30698 98656 75249 59331

         DESTROY AFTER USE                   DESTROY AFTER USE

+                                   +                                   +
```

Summary ▲

Create pairs of one-time pads with truly random digits, one copy for sender and one copy for receiver. To encipher a message, convert the plaintext into digits with the help of the conversion table. Write the one-time pad underneath the converted plaintext, but skip the first group of the one-time pad. Subtract the one-time pad from the plaintext, without carry. Put the skipped first group of the pad in front of the ciphertext message to tell the receiver which pad was used. Destroy the pad after enciphering.

To decipher a message, check the first group of the ciphertext to see which one-time pad was used. Write the proper one-time pad underneath the ciphertext but skip the first group of both ciphertext and pad. Add ciphertext and one-time pad together without carry. Convert the resulting digits back into plaintext with the help of the conversion table. Destroy the pad after deciphering.

1. Create one-time pads with truly random digits
2. Never ever use a one-time pad more than once
3. Destroy the one-time pad immediately after use

More about one-time pad on this website ▲

- NEW **Guide to Secure Communications with the One-time Pad Cipher** How set up secure communications with one-time pad
- **One-time pad** about one-time pad and its history
- **Numbers Stations** about shortwave broadcasts of encrypted messages
- **Spies and Numbers - Here to Stay** The use of one-time pads in espionage
- **Cuban Agent Communications** Paper on Cuban numbers stations, Cuban agents in the U.S. and the errors they made
- **Is One-time Pad History?** About the usefulness of one-time pad encryption