Cipher Machines & Cryptology

http://users.telenet.be/d.rijmenants

THE COMPLETE GUIDE TO
SECURE COMMUNICATIONS
WITH THE
ONE TIME PAD CIPHER

DIRK RIJMENANTS

Abstract: This paper provides standard instructions on how to protect short text messages with one-time pad encryption. The encryption is performed with nothing more than a pencil and paper, but provides absolute message security. If properly applied, it is mathematically impossible for any eavesdropper to decrypt or break the message without the proper key.

Keywords: cryptography, one-time pad, encryption, message security, conversion table, steganography, codebook, message verification code, covert communications, Jargon code, Morse cut numbers.

Version 022 (17 Feb 2012)

Contents

I. Introduction

One-time pad encryption is a basic yet solid method to protect short text messages. This paper explains how to use one-time pads, how to set up secure one-time pad communications and how to deal with its various security issues. It is easy to learn to work with one-time pads, the system is transparent, and you do not need special equipment or any knowledge about cryptographic techniques or math. If properly used, the system provides truly unbreakable encryption and it will be impossible for any eavesdropper to decrypt or break one-time pad encrypted message by any type of cryptanalytic attack without the proper key, even with infinite computational power (see section VII.b)

However, to ensure the security of the message, it is of paramount importance to carefully read and strictly follow the security rules and advice (see section VII). Do not use one-time pads before reading this paper from start to end!

Why should you use encryption?

Cryptography can protect the secrecy of your private communications. Privacy is a natural right that allows personal autonomy, while ensuring your democratic freedoms of association and expression. The definition of privacy differs among cultures and countries. Some governments impose restrictions or prohibit the use of strong cryptography by their citizens because it limits government surveillance. The fight against crime and terrorism are popular excuses to blur the boundary between a legally authorized surveillance and blunt intrusion in people's privacy. More about the legal issues regarding cryptography is found in section VII.j.

Common notations

Some notations, used in this paper: *cryptography* and *cryptanalysis* are the sciences of making and breaking codes. The readable and unprotected message is called *plaintext*. *Encryption* or *enciphering* is the process to make a message unintelligible by applying an *algorithm* under control of a key. The result of encryption is called *ciphertext*. *Decryption* or *deciphering* is the process to turn the ciphertext back into readable plaintext with the help of the proper key.

II. The One-time Pad

To perform one-time pad encryption we need a key, called one-time pad. A one-time pad can be a single sheet, a booklet or a strip or roll of paper tape that contains series of truly random digits. A one-time pad set consists of two identical one-time pads, one pad called OUT and one called IN.

To establish one-way communications, you only need one OUT pad for the sender and one IN pad for the receiver. To communicate in both directions, you need two different one-time pad sets: person A has an OUT pad of which person B has the IN copy, and person B has another OUT pad of which person A has the IN copy. Never use a single pad to communicate in both directions to avoid the risk of simultaneous use of the same pad sheet!

The use of multiple IN copies of a pad, to enable more than one person to receive a message, is possible but not advisable. Multiple copies pose additional security risks and should only be used in a strictly controlled environment. Never use multiple OUT copies of a pad, as this will inevitable result in simultaneous use of the same pad and the risk of non destroyed copies of a pad.

One-time pad encryption is only possible if both sender and receiver are in possession of the same key. Therefore, both parties must exchange their keys beforehand. This means that the secure communications are expected and planned within a specific period. 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 period, up to several years.

In section VII.b you will find instructions on how to create one-time pads. Carefully read these instructions before creating your own one-time pads. The quality of the one-time pads is a vital part of the message security!

Example of a one-time pad sheet:

```
            OUT 0001

68496 47757 10126 36660 25066
07418 79781 48209 28600 65589
04417 18375 89891 68548 65437
96152 81871 38849 23191 35777
59888 98186 01174 19456 73831
74345 88365 39797 08166 97776
96571 53718 56970 37940 60539
91243 74502 87465 41884 44533
72057 94612 35304 29054 33274
48090 79776 45366 46827 11680

       DESTROY AFTER USE
```

Note that there are also one-time pads with letters. These pads are only suitable to encrypt letters-only text. For reasons of flexibility, the one-time pad system in this paper uses one-time pads with digits.

III. Message Preparation

When composing your message, use short concise sentences and avoid repetitions. Omit spaces where it does not affect readability. Use abbreviations where possible. If available, use a codebook to reduce message length (see section VI). Do not use names of persons or places if the origin or destination of the message, or the message itself, clarifies which names are meant. Never use a fixed structure or format in the message. The message should not exceed 250 digits after conversion (approx. 180 characters). Divide larger messages into parts of 250 digits and encrypt each part with a new one-time pad key.

Before we can calculate the ciphertext, we must convert the plaintext into a series of digits with the help of a so-called checkerboard. The frequently used letters are represented by a single-digit value. All other characters are represented by a double-digit value. The table is optimised for English (more about these tables is found in Appendix A). Note that this conversion on itself provides absolutely no security and must always be followed by the proper encryption!

The character-to-digits checkerboard and its printable version:

CODE	A	E	I	N	O	T	CT NO 1 ENGLISH		
0	1	2	3	4	5	6			
B	C	D	F	G	H	J	K	L	M
70	71	72	73	74	75	76	77	78	79
P	Q	R	S	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	( )	(+)	(-)	(=)	REQ	SPC
90	91	92	93	94	95	96	97	98	99

```
CONVERSION TABLE NO.1 EN

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

Spaces are represented by 99 (SPC). A comma and apostrophe are both represented by 93('). Figures are always written out three times to exclude errors and they are preceded and followed by 90 (FIG). If required, the Request code 98 (REQ) can be replaced by a question mark. Punctuations are allowed within figures. Some examples:

```
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N    N  Y  (.)
79 2  2  6  3  4  74 99 1  6 90 111 444 90 80 79 99 3  4 99 4  88 91

S  I  Z  E  =      3  .   5     F  E  E  T
83 3  89 2  97 90 333 91 555 90 73 2  2  6
```

The codebook prefix CODE (0) precedes three-digit codebook values (see section VI about the codebook). Spaces are unnecessary before and after codebook codes. The use of a codebook is optional but can reduce the message length and transmission time considerably. You can always omit the use of a codebook if the receiver does not posses a copy of the codebook.

In the next example, we use the codebook values PASSPORT (587), FLIGHT (352), UNABLE-TO (884) and FERRY (343) from the codebook in section VI.

```
REQUEST  N E W  PASSPORT  F  O R  FLIGHT (.) UNABLE TO  U  S  E  FERRY
98       4 2 86 0587      73 5 82 0352   91  0884       84 83 2  0343
```

Notice that we only need 34 digits for a text with 43 characters, which is a very efficient 0.8 digit/letter ratio, compared to an average 1.3 ratio in a text conversion without codebook.

IV. Encryption

Before we start the encryption process, we must tell the receiver which one-time pad is used. Therefore, the first group of the one-time pad is used as key indicator at the beginning of the message. Never use the first group of the pad in the encryption process! Never send a one-time pad serial number along with the message because this would reveal the number of messages that were sent, and their order.

To encrypt the message, write down the digits of the converted text in groups of five digits and write the digits of the one-time pad underneath them. Always complete the last group with full stops (9191…). Do not forget to skip the first group (key indicator) of the one-time pad!

Subtract the one-time pad digits from the text digits, digit by digit, from left to right. The subtraction is performed without borrowing (e.g. 5 - 9 = [1]5 - 9 = 6). In the following example, we use the message from section III and the one-time pad from section II.

```
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N    N  Y  (.)
79 2  2  6  3  4  74 99 1  6 90 111 444 90 80 79 99 3  4 99 4  88 91

Plaintext : KEYID 79226 34749 91690 11144 49080 79993 49948 89191
OTP Key(-): 68496 47757 10126 36660 25066 07418 79781 48209 28600
            -----------------------------------------------------
Ciphertext: 68496 32579 24623 65030 96188 42672 00212 01749 61591
```

Below, the complete ciphertext, rearranged in the standard format of five groups per row. If the message is sent by radio, in voice or Morse, or by telephone, it is recommended to relay all groups twice to avoid errors (e.g. 68496 68496 32579 32579...). If the receiver has call sign 401, the message could look like this:

```
401 401 401

68496 32579 24623 65030 96188
42672 00212 01749 61591
```

Important: always destroy the one-time pad sheet immediately after finishing the encryption, even when it still contains unused groups. A new message should always be encrypted with a new sheet. NEVER reuse a pad!

V. Decryption

To decrypt the message, check its first group (the key indicator) against the first group of your one-time pad, to make sure that the proper one-time pad is used. Write the one-time pad digits underneath the ciphertext and add ciphertext and one-time pad together, digit by digit, from left to right without carry (e.g. 9 + 6 = 5 and not 15). Remember that the first group is not used during the decryption process, and only serves as key indicator.

```
Ciphertext: 68496 32579 24623 65030 96188 42672 00212 01749 61591
OTP Key(+): 68496 47757 10126 36660 25066 07418 79781 48209 28600
            -----------------------------------------------------
Plaintext : KEYID 79226 34749 91690 11144 49080 79993 49948 89191
```

After decryption, the resulting digits are re-converted back into plaintext letters with the help of the conversion table. It is easy to separate the single-digit from the double-digit values: if the next digit is between 1 and 6, it represents a single-digit value. If the next digit is 7, 8 or 9, it represents a double-digit value and you must add the following digit to complete that double-digit value. If the next digit is 0 (CODE), it will be followed by a three-digit code that represents a word or expression from the codebook. Remember that figures are written out three times.

Our message, re-converted into text with the conversion table:

```
79 2  2  6  3  4  74 99 1  6 90 111 444 90 80 79 99 3  4 99 4  88 91
M  E  E  T  I  N  G     A  T     1   4     P  M     I  N    N  Y  (.)
```

Written out: MEETING AT 14 PM IN NY

Important: always destroy the one-time pad sheet immediately after decryption!

Encryption & Decryption Quick Summary

To encrypt, convert the message into digits and subtract (without borrowing) the one-time pad from the text digits. Skip the first group of the one-time pad during the encryption process and use it as key indicator at the beginning of the ciphertext.

To decrypt, verify whether the first group of the ciphertext (key indicator) is identical to the first group on your one-time pad. Write the one-time pad underneath the ciphertext digits and add both together (without carry). Convert the resulting digits with the conversion table back into readable text.

ALWAYS DESTROY THE ONE-TIME PAD IMMEDIATELY AFTER USE!

NEVER USE A ONE-TIME PAD MORE THAN ONCE!

VI. The Optional Codebook

The codebook table no. 1 (see also Appendix B) contains various words that would normally require more than four digits to convert. The words are listed in alphabetic order. The non-consecutive values are selected carefully in order to detect single-digit errors and in most cases double-digits errors during decryption (an error results in a non-existing value). The codes 947 through 992 are available for local geographical names, specific technical expressions or names. The codebook prefix CODE (0) must precede each codebook value!

CODE TABLE NO.1

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 .....
208 COORDINATE	451 LOCATE	703 REPEAT	956 .....
217 COUNTRY	460 LOCATION	712 RESERVATION	965 .....
226 COVERT	479 MAIL	721 ROUTINE	974 .....
235 CURRENT	488 MEETING	730 SATELLITE	983 .....
244 DANGER	497 MESSAGE	749 SHIP	992 .....

Some words in the codebook are extendable or changed by addition of one or more characters with the help of the conversion table: the plural of 0596 (PERSON) will be 05966 (PERSONS). The past perfect of 0686 (RECEIVE) will be 068672 (RECEIVED), and 0901 (VERIFY) will be 090175 (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).

Of course, you can create a codebook with your own words, phrases or expressions, tailor-made to your specific needs. Maintain the special codebook value sequence in order to preserve the error check ability. It is not advisable to use consecutive values (001, 002, 003 …999) because a single-digit error during communications or decrypting would produce a completely different codebook word or phrase. A customizable codebook for 100 words or phrases is available in Appendix C. Another customizable codebook, for 220 words or phrases, is available in Appendix D. There is a codebook digit sequence for 807 words and phrases, to create a large codebook, available in Appendix E. All number sequences are composed in such way that they always detect single-digit errors and in most cases double-digit errors. Don’t forget the prefix CODE (0).

VII. Security Rules and Advice

Although one-time pad encryption seems simple and straightforward, there are several important rules that are essential for the security of the message. Not following these rules will always result in the compromise of the message and the one-time pads. Even a small and seemingly insignificant mistake can result in unauthorized decryption of the messages. These rules are not negotiable!

History, court documents and intelligence records have shown many examples of intercepted and decrypted one-time pad communications. Such cases are often mistakenly referred to as cases where one-time pads were broken. In reality, those messages were not actually broken but compromised because somebody at some point did not follow the rules. Often, the users were thoroughly instructed beforehand but they believed that those little details did not matter. They were wrong and paid dearly for their negligence!

However, a one-time pad encrypted message is truly unbreakable if the rules are followed. It will always be and always remain unbreakable, even for the brightest cryptologists with the fastest super computers until the end of times, simply because it is mathematically impossible to break one-time pad. Absolute security is a reason to opt for one-time pad. However, safeguarding that level of security is not without effort. Read the following information carefully!

a. Use of Computers

The improper use of computers for cryptographic applications is the most common and fatal error. Normal computers are NEVER suitable for crypto applications, despite many commercial firms selling crypto software for personal computers. Only dedicated computers, stored on a secure locations, or special purpose devices are suitable for cryptographic purposes. There's no such thing as a secure personal computer. Those who contradict this either have no clue about security or have a hidden agenda (commercial profit, surveillance…).

The one-time pad system should be used with nothing more than a pencil and paper, and for good reasons. There are some critical security issues to consider when a computer or other peripheral devices are used. Readable data can, and most often will, either reside unintentionally on computers, in the memory, in temporary or swap files on the hard disk, or in memory buffers of peripherals. No single network connected computer is secure and will always be vulnerable to malicious software, spy ware or intrusion by skilled hackers or professional organisations.

If an eavesdropper cannot decrypt it, he will definitely try to retrieve it from the targeted computer, either remotely by spy ware, by hacking into the computer, or physically by (surreptitious) examination of the computer or its peripherals. He will get the data before encryption or, when already encrypted, by analysing the hard disk for data remanence after encryption. Secure file deletion software can prevent or remove (wipe) remanent data by overwriting it. Some well know software is WIPE or ERASER.

Nonetheless, court documents of espionage cases revealed that sensitive data was recovered successfully from computers, despite wiping software (malfunctioning software, incorrect or negligent use). In 95 percent of the cases, intelligence agencies don't even bother trying to decrypt data. They simply retrieve the readable data from the computer before encryption, without the targeted person ever noticing.

It is essential that you always use a dedicated stand-alone computer (preferably a small laptop or netbook) that is never connected to a network (if possible, remove its network card and lock the casing). The computer must be stored permanently in a physically secure place (e.g. safe, armoured room) to restrict unauthorized persons from accessing the computer.

As you can see, there are enough reasons not to use a computer: the security measures are difficult to apply, expensive and not full proof. Since one-time pad encryption is most suitable for a small volume of message, it is recommendable to generate the one-time pads and perform encryption and decryption manually.

b. Creating One-time Pads

A standard one-time pad sheet contains 250 digits in groups of five digits, which is enough for a message of approximately 180 characters. The first group of five digits on each sheet serves as key indicator and must be unique for that particular set of sheets. All digits on each pad must be truly random. The randomness is an essential part of the security of the encryption process.

Do not use nor derive digits from a phone book, technical publications, books, websites or from any series of digits that is printed or published in any way, anywhere. These are all but random, and certainly not secret. Do not use values that are not within the range 0 through 9. Humans neither are unsuitable to produce randomness. They unconsciously behave according to well-defined rules. If they think, “I should not pick a 6 because I already just wrote a 6”, the next digit is not random, because it has followed a rule. Don’t just pick some digits for a key.

If a truly random key is subtracted from a given plaintext by modulo 10 (without borrowing), then each resulting ciphertext digit will also be truly random. Consequently, there is no relation between the individual truly random ciphertext digits, and the ciphertext does not reveal any information whatsoever about the plaintext or about other parts of the ciphertext. The process is mathematically irreversible without the proper key.

THE SECURITY DEPENDS ENTIRELY ON THE QUALITY OF THE RANDOMNESS

There are various ways to generate series of truly random digits. You can generate random digits with a computer. However, such systems must be selected with care and they create additional security risks (see VII.a regarding the use of computers). The best option is to use a hardware-based true random number generator (TRNG) of which the output is derived from a random noise source. These are available as PC card or as USB device. Only purchase generators from well-known firms (Mils Electronic, ID Quantique, true-random.com...). Today, some microprocessors have included a hardware true random generator, using thermal noise or variations in electrical characteristics of the electronic components on the processors. In such case, the computer itself can provide quality randomness.

If you generate random digits purely with software, you will never have truly random digits, which is one of the conditions for unbreakable encryption. A computer program will always be deterministic and by definition predictable. If you do want to use a software-based generator, use only a crypto-secure random number Generator (CSRNG), initialised with a very large random seed, derived from a random source like mouse movements and random process time measurements. Again, this last option could produce a cryptographically secure series of digits that is practically unbreakable, but will never be theoretically truly unbreakable.

If you have to encrypt a low volume of messages, you can generate a small number of one-time pads manually. Although time consuming, it is easy to obtain a high quality of randomness.

One method is to use five ten-sided dice. Each new throw gives a new group of five truly random digits. Ten-sided dice are available in many toy stores. Never simply use normal six-sided dice by adding the value of the dice and discarding two values. 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 that the values 2 or 12). Instead, use one black and one white die and assign a value to each of the 36 combination, 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.

GENERATING TRUE RANDOM (0 – 9) WITH BLACK AND WHITE DICE

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 also time consuming method is a lotto system with balls that are numbered from 0 to 9. Make sure to mix an extracted ball again with the rest of the balls before extracting a new ball.

c. Storage of One-time Pads

One-time pads are usually printed as small booklets that contain a large numbers of one-time pad sheets. The top sheet is torn off and destroyed after a message is encrypted. The pads are printed in various formats and sizes. If both sender and receiver can store their pads securely, these will be normal sized booklets. When used in covert circumstances, the most practical pads are printed with a very small font (font size 4 or less) on very small thin paper sheets. These are easy to hide and destroy, although one should be very careful in hiding them (see VII.f).

One-time pads can be stored in tamper-proof sealed containers (plastic, metal or cardboard) to prevent, or at least detect, unauthorised disclosure of unused series of digits. It is not advisable to store one-time pads on a computer, memory stick or CD (see VII.a regarding computers). Erasing data on these carriers is very problematic and total destruction of used one-time pads is never guaranteed. Specialized techniques exist to retrieve computer data, even after deletion or overwriting. In critical situations, it is harder to quickly dispose or destruct a memory stick, floppy disk or compact disk than to, for example, eat a small paper sheet.

Always distribute the one-time pads physically, either personally or by a trusted courier. Never send one-time pads electronically because there is no method of communications that provides the same level of security. Encryption with a strong crypto algorithm, prior to sending them electronically, is useless and will compromise the one-time pads. Doing so will lower the pad’s security from unbreakable down to the security of the used encryption.

The most important part of the one-time pad scheme is a secure key management. If the key is not 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.

Immediately after creation, a one-time pad key pair must be serialised and registered. There should be a centralised (star topology) registration and distribution in order to know who has what 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 all remaining copies of that key must be destroyed immediately. Never use a one-time pad more than once! If you do so, basic cryptanalysis will break all messages, encrypted with the reused one-time pad.

Of course, one-time pad encryption does not always have to be that complicated. It is also very suitable for one-time occasions. Although you normally might never need encryption, you could encounter an emergency where you need secure communications, by telephone, e-mail or regular mail. A lost PIN code during the holidays, someone needs access to the safe in your office or your home burglar alarm needs a reset code. Everyone remembers a situation where he had to give some information but felt uncomfortable with using a phone, a letter or e-mail.

One-time pad encryption offers an elegant solution to convey sensitive information in such one-time situations. You only have to carry a single small emergency one-time pad for one-time use. Of course, you also need a confidant, a family member or employee, who also has a copy of that pad. Such emergency pad could contain a small set of random digits and a little conversion table. Printed in a font size 3 or 4, the pad would measure a mere one by one inch. You could pack and seal it in plastic. You could store the pad in a medallion, safely hanging on your necklace, or inside your watch (underneath the back cover). In case of emergency, you phone home, let them write down a few groups of digits and tell them to get the pad. No elaborate and complicated security measures are involved.

d. Compromise of one-time pads

The compromise (no longer being secure) of a one-time pad or a booklet will endanger all communications, made with those one-time pad sheets. Therefore, it is essential that each sheet is destroyed immediately after used, to prevent the compromise of those messages that are already sent.

A one-time pad is always compromised when:

- used more than once
- not destroyed after use
- not securely stored at any moment in the past.
- a user is suspected to have violated security rules
- exposed intentionally or unintentionally to other people.
- lost or no proof of proper destruction
- it is unknown whether the one-time pad is compromised or not

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

e. Secure Encryption and Decryption

Never use a computer to type a plain message or to encrypt or decrypt (see VII.a). Instead, use a single piece of paper on a hard surface to write down the message and perform the calculations. Destroy that paper and the used one-time pad key immediately after you finished. Although one should not become paranoid, keep in mind that writing onto the first page of a bloc or onto a paper on top of a magazine or newspaper always leaves minor impressions on the underlying paper. The most secure and convenient method to destroy keys is simply to burn them.

Check you encryption before sending the message. A single error could make the message unreadable or result in critical mistakes during decryption. Once encrypted, you can store the ciphertext anywhere you like. It will stay unbreakable. However, for reasons of deniability, it is not recommended to store ciphertext on a computer or any other easily accessible medium.

f. Message Security

Unbreakable encryption does not provide absolute message security. Message security indeed involves secure encryption but also includes various measures that prevent the opponent to retrieve information that helps him to decrypt the message.

If sender and receiver are in a safe environment, free from risk of surveillance, intrusion of the privacy or prosecution, they can send their encrypted communications by any means, even insecure. It does not matter if someone intercepts the encrypted message. The message is unbreakable anyway. Unfortunately, this ideal world hardly exists. Since it is mathematically impossible to break a one-time pad encrypted message by cryptanalysis, any eavesdropper will try to get his hands on either the original readable message or the one-time pad key, used to encrypt that message.

In the real world, the eavesdropper will attempt to retrieve the identity and location of sender or receiver. Identification of the involved persons is the first step in reading their communications. The mere identification of a person who sends or receives encrypted communications, even unintelligible, might have serious consequences under an oppressive regime. Once identified, the eavesdropper can start surveillance and use technical means to retrieve information from that person's computer or perform a surreptitiously search of his house to copy one-time pads that are will be used in the future. The person might never know his security is breached and that his messages are read.

The message itself, even unintelligible, might give clues about who is sending the message, about its contents and to whom it was sent. This technique is called traffic analysis. The amount of messages, their length or sudden change in length might link that message to a particular event that occurred prior to, or after the message was sent, leading to the involved persons. To avoid traffic analysis, you can send each message with a fixed length of 250 digits by simple appending the unused random one-time pad digits at the end of the ciphertext. Any eavesdropper would observe that all messages have the same length and he has no idea of the actual message length.

Of course, physical security is also part of message security. If a (surreptitious) house search, theft or seizure are likely or possible, any documents, computers or other data carriers that contain one-time pads, readable messages, ciphertexts, instructions (conversion table, codebook) should be well hidden or stored on another location, impossible to detect by surveillance or a search. Again, miniature paper one-time pads have the advantage over digital carriers that they are easy to hide.

Tiny and thin sheets could be stored inside a power socket, a TV remote control, a kitchen knife's handle, inside toys or between layers of a book cover. One's imagination is the limit. In event of an expected search, they are easily destroyed by burning them. If you hide one-time pads, you

should always use some system to detect the compromise of the hiding place. This could be a very accurate positioning of the pad in the hiding place, or some tiny object (hair, grain of sand or dust particle) at a specific location, that is moved accidentally by the ignorant intruder.

This is a good moment to explain that, in case the use of one-time pads is suspected, a house search could mean the total and thorough dismantling of the house and every single object inside, up to the tiniest parts of furniture, coffee machines or even the removal of all plaster on the walls, to mention a few. This sounds funny, unless you are innocent… or when you actually hide pads.

Also, never talk in public about the fact that you use one-time pad encryption and never mention the words "one-time pad". Select one or more code words to refer to one-time pad communications. Tell your friend to bring along some "*marshmallows*", or to send you a new '*baseball cap*". Do not call him by phone and tell him you ran out of one-time pads.

Now that we understand the ways in which our manner of communication influences message security - along with our personal security - we can take measures to avoid detection of our communications.

g. Covert Communications

If the opponent has the technical means for surveillance, we need to communicate covertly or disguise our message. Covert communications are a most difficult issue. Telephone, mobile or satellite phone, voice or text message, paper mail, e-mail, the Internet and other network based digital communications are always to be considered absolutely insecure. They enable identification of both sender and receiver. These channels should never be used to communicate covertly.

Today, all electronic communications are stored for longer periods. A phone call or mobile phone's text message are no longer moments in time. These are digital events, permanently residing in databases, ready to be exploited. An anonymously bought pre-paid card will link that particular mobile phone or phone boot to a call or text message. If either pre-paid card or mobile phone, used for covert communications, is reused for other purposes, it will be possible to link both events and, combined with geo-location, can lead to both participants of the call. Be aware that the trick of breaking off the conversation before they can trace you is Hollywood fantasy in today's digital world. A call is traceable from the very first second, even long time after the call ended, just as e-mail traffic is. All these cards, phones and Internet connections are only suitable for one-time use.

Publicly available systems could be suitable to communicate anonymously. Some examples are computers in a cyber café or library (of course without need for registration) or a public phone (with anonymously bought pre-paid card). We can post or read message on Internet forums or on random on-line guest books, with a cyber-café computer. However, although publicly available communications might be anonymous, it remains possible to retrieve time and location of these communications. In such case, a witness or security camera could link that particular time and place to the user of that public phone or computer.

Shortwave radio is an ideal way to receive messages covertly over large distances, either by voice, by Morse or a modulated signal (which requires special receiving equipment). Morse code is a most suitable method to convey the message digits. It enables good reception, even under very poor conditions, and it is easy to learn. If the message contains only digits, the use of so-called *cut numbers* (see appendix G) can reduces the transmission time considerably.

Having a simple household shortwave radio is not suspicious. Of course, one must avoid storing the receiving frequency in the radio preset memory or in its "last used frequency" memory. Although technically possible, it is hard to locate someone who receives a particular broadcast. Receivers use local oscillators to tune to the desired frequency, and these oscillators

unintentionally emanate weak spurious signals. These signals are traceable only with very sensitive equipment in the vicinity of the receiver. Nevertheless, it is a good habit to keep distance, something that might be difficult in cities or buildings where surveillance close by is possible.

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 permits surveillance and interception of many signals simultaneously on several wide frequency ranges. The use of burst-transmission (transmitting a message at high speed) 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, spy gear you do not want to be caught with.

h. Steganography and Deniability

As you can read, it is all but easy to communicate truly anonymously in today's high-tech and fully digitized world without leaving any trace. Another way to convey the message is to do this openly, but to disguise the message in such way that the eavesdropper does not know that the message has been sent. This technique is called steganography (lit. hidden writing) and enables both sender and receiver to fully deny the existence of encrypted communications.

Always use Steganograhy in combination with encryption. Never hide plaintext in a message. When steganography is suspected, or even when the method of hiding is known, an attempt to extract encrypted data from the suspicious message will only produce unintelligible nonsense, just as any innocent text would. The message remains deniably. However, an attempt to extract a hidden but non-encrypted text could produce readable information. Protect before hiding!

There are various ways to hide ciphertext numbers in a seemingly innocent letter or e-mail. Of course, simply inserting strange sequences of digits or some illogical values will draw suspicion. In this paper, we use a so-called *Jargon code*, where 10 sets of 22 words correspond to a particular digit. The words are used to compose a readable and innocent looking text. The large number of words that represent a single digit ensures flexibility and variation in the composed text. An example of a digit-to-words table is available in Appendix F, at the bottom of this document.

Any of the 22 nouns and adjectives, assigned to a particular digit, can be selected to compose the text. To extract the hidden digits from the seemingly innocent 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 use our digit-to-words table from Appendix F to hide some digits in a text. It is allowed to use the plural of certain words (movies, cars, houses...) as long as the word stays intact, to avoid confusion. Occasionally, but not too often, ciphertext digits can be inserted directly in the text wherever this looks unsuspicious ("It took me 40 minutes to...").

The ciphertext groups 68496 32579 24623 from our example message, hidden inside a text:

"Last evening, I cleaned up my fridge. The kitchen was a mess. I dropped a brik of tea and even discovered a very smelly fish. Too late to put that one in the freezer! Meanwhile, I'm back in my lazy chair with a cup of coffee, listening to some music. I just read in a magazine about a recipe with cheese and pasta. Maybe something for next Sunday. A nice Italian wine would make it complete. I'll surprise my mother with that one!"

Of course, in this example, the digit-words are underlined for demonstration purposes only. We now have a nice and innocent looking piece of text. Make sure to compose a text that makes

sense. A large and varied set of words facilitates the composing of a meaningful text. Writing about a trip you never made or about a family member or your dog that doesn't exist could compromise your story. Writing about things that you would like to have or to do, or about things in the future is safer because such information is harder to verify. Avoid unintentional use of table words, as this would add a wrong digit and could render the text undecipherable. Double-check your work!

The receiver checks each noun and adjective in his word-to-digit table. If the word appears in his table, he writes down the corresponding digit. When finished, he decrypts the re-compiled ciphertext with the proper one-time pad, and re-converts the digits into readable text.

This method provides much flexibility, although it might take quite a few sentences to hide a large number of digits. More words per digit in the table gives more flexibility and variation. Indeed, with only a few words per digit, a text that contains the word “sandwich” more than 35 times would look very odd.

Of course, you should compose your own table with your own set of words, some of them possibly related to your specific environment so that the subject of the innocent letter matches your personal world. You can also use more than 22 words, which is even better, although too many words might become impractical. Although there is nothing illegal to a paper with a list of words, the digit-to-word table should be kept secret as its discovery might ring a bell.

With this method, the hidden message is fully deniable. There is no way to prove the existence of a message inside the innocent looking letter without knowing the method of extraction, the proper set of words and the proper one-time pad key. Linguistic analysis of the letter could show differences with other ‘clean’ letters, written by the same author. This however merely proves that the author has a slightly erratic writing style, a lack of inspiration or that he had one glass of wine too much in his boots when he wrote his letter.

Given the fact that, in today's digital world, virtually all means to communicate are prone to eavesdropping, we have a safe solution to send messages by postal mail, e-mail, on-line accounts, Internet forums or any insecure channel. This is especially interesting in countries where the use of encryption is prohibited and a series of five-digit groups draws attention like a red scarf on a bull. The conversation itself however stays detectable and you will need a good excuse for what you wrote and to whom you wrote it.

i. Common Mistakes

To err is human. Unfortunately, mistakes with one-time pads are usually fatal. Below a list of the seven most common mistakes that people make when they use one-time pads.

1. Bad Randomness

The most dangerous error is the use of non-random digits for the key. This is an error you cannot see with the naked eye, and could even remain undiscovered when the ciphertext is examined. Nonetheless, cryptanalysis can and often will exploit this flaw to successfully decipher a message.

2. Not destroying used keys

Humans are collectors. They keep keys that should have been destroyed, for various reasons (the co-called “in case of…” syndrome). Keeping a used key is a very bad idea. If the key is not destroyed, the message is not unbreakable and is waiting to be deciphered by those who find the key.

3. Insecure storage of keys

If you store your keys in a five-dollar money box, you will have a five dollar security level. If you store your keys in a real safe, you message is unbreakable when the safe is unbreakable. Unfortunately, safes are not unbreakable. If you do not securely store or hide your keys, they are compromised the moment you leave your house or office.

4. Insecure computers and alike

Computers are a security nightmare. Everything leaks out and everybody can get in. It is a very common mistake to assume your computer is secure. It is not because your anti-virus software cannot find anything, that your computer is not infested with spy ware. Today’s photocopiers and multi-functional printers also have a processor, store each copy also on their own hard disk and they are often connected to a network. Do not use those to print or copy confidential information.

5. Multiple copies of a plaintext

If you have stored or processed the unprotected plaintext on any type of carrier (computer, USB stick, photocopier, paper…), the message is no longer secure, unless you apply the same strict physical security rules on that carrier as you would apply on your keys. Otherwise, there is a serious risk that the plaintext is disclosed, possibly without you even knowing it.

6. Loose lips and false confidence in people

People love secrets, but secrets are only fun when you share them. Loose lips can be fatal. Unbreakable encryption is useless when you tell the secret to others. Humans are unpredictable and you can never know what people do with the information you shared with them. Do not underestimate the primal urge to share secrets! For some people it is almost irresistible. There is a simple yet very effective rule to keep a secret: only share the secret or confidential information on a “need to know” basis. Does he really need to know? If not, do not tell him!

7. Not following the rules

Finally, some people are cocky and do not follow the security advise of others. They think they are smarter and they believe they have a better way to do things. Stubborn people often have amnesia: they forget that other people have spent a lot of time making up rules and procedures. Do not start improvising to get around seemingly useless, stupid or time-consuming rules.

j. Legal Issues and Personal Security

Cryptography protects the right to privacy and the right to communicate confidentially. Secure communications can protect one's intimate private life, his business relations, and his social or political activities. These basic rights are written in the constitution of many, but not all countries. Of course, it is illegal to use cryptography for criminal or terrorist purposes. This does not mean that the use of cryptography should be illegal. Just as with weapons, a knife or a crowbar, it is not because you could use these objects for illegal purposes that they should be regarded as illegal. It is useless to make cryptography illegal. Criminals simply don't care about the law. If you outlaw cryptography, only outlaws will have privacy.

However, even the most liberal and democratic countries have laws that control the use of cryptography and some countries have stricter laws than others. Many governments are reluctant to permit the use of cryptography by their citizens because it limits the government's surveillance capabilities. The laws are often a balancing between the protection of the individual privacy and a nation's security or its the fight against crime.

Democratic countries tend to permit cryptography for personal use and have legal mechanisms to bypass the right to privacy with a court order in case of a criminal investigation or a threat to the nation. The boundaries between lawful surveillance and state organized invasion of privacy is often a subjected to discussion, even in democratic countries.

Depending on the country, laws on cryptography can restrict specific types of cryptography partially or allow only government licensed systems, limit the strength of the encryption or demand key escrow. Some laws can force someone to hand over the decryption keys following a judicial warrant and there are laws that restrict the import or export of cryptographic software, equipment or knowledge, or even regard export of cryptography as weapons export.

Violating these laws can have serious legal consequences, ranging from penalties over prosecution up to imprisonment. In countries with oppressive and dictatorial regimes, democratic rights and laws on privacy are often non-existing or aimed solely to protect the ruling regime. In such countries, citizens are often forbidden to use cryptography and legal consequences can range from life imprisonment to death penalty.

Inform yourself about the legal restrictions on cryptography in your country or in the country where you are planning to use it. The use of cryptography, and especially the unbreakable one-time pad encryption, described in this paper, could result in a criminal investigation, prosecution and severe penalties. In some countries, being caught with one-time pads or sending encrypted messages could cost you your life. Think carefully before you start using one-time pad encryption. It is very easy to encrypt and decrypt messages with one-time pads, but very hard to follow all the necessary strict rules that are vital to protect your and other people's personal security.

The use of one-time pads is a balance between the protection of communications secrecy and the risks involved in using it, depending on the country where you reside. If you have any doubt about your ability to cope with the security issues or risks involved, do not use encrypted communications!

VIII. Appendices

Appendix A

Straddling Checkerboards

A practical and visually easy method to convert text or symbols into digits is the so-called straddling checkerboard. This is a table with labelled columns and rows. Column digits above empty cells are also used to label the remaining rows. A letter from the first row is converted into the digit labelling its column. The letters from the second and third row are converted into a two-digit value, composed by the row and column digits. Allocating the most frequent letters of a language to the top row will reduce the length of the converted text considerably.

The first example, which is optimised for English, is the simplest version, easily memorised by its top row words AT ONE SIR. Column digits that represent empty cells in the top row are used to label the remaining rows. Here, T = 1, N = 4, F = 23 and U = 62. F-L switches between letters and figures and / is used as word or sentence separator.

	0	1	2	3	4	5	6	7	8	9
	A	**T**		**O**	**N**	**E**		**S**	**I**	**R**
2	**B**	**C**	**D**	**F**	**G**	**H**	**J**	**K**	**L**	**M**
6	**P**	**Q**	**U**	**V**	**W**	**X**	**Y**	**Z**	**F-L**	**/**

For each additional empty cell in the top row, we can add a full row, thus creating 10 additional cells. The next example, also optimised for English, has four empty cells, allowing four rows of two-digit values. In addition, some cells contain the most frequent English digraphs. Just as the top row letters, these digraphs reduce the total number of digits that are required to convert a text.

CODE	**A**	**E**	**I**	**O**	**T**				
0	**1**	**2**	**3**	**4**	**5**				
AN	**B**	**C**	**D**	**ED**	**EN**	**ER**	**F**	**G**	**H**
60	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**
HA	**HE**	**IN**	**ION**	**J**	**K**	**L**	**M**	**N**	**ON**
70	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**
P	**Q**	**R**	**RE**	**S**	**TH**	**U**	**V**	**W**	**X**
80	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**
Y	**Z**	**(.)**	**(,)**	**(:)**	**(/)**	**($)**	**(-)**	**F-L**	**SPC**
90	**91**	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**

Of course, many other tailor-made Checkerboard designs are possible. The goal is always to reduce the message length. The table could contain more trigraphs or even frequently used small words or expressions. Always use combinations that are more efficient than the letters separately (f.i. digraph TO holds no benefit because T and O together also use two digits). You could also allocate both letters and symbols to a single value, controlled by an upper/lower-case cell.

Note that some encryption schemes use checkerboards with scrambled alphabets and/or scrambled labelling. This, however, is not necessary when the conversion is followed by a one-time pad encryption, because the encryption is unbreakable anyway.

Language and letter frequency optimized checkerboards

French
(memorized by the keyword SAINTE)

CODE	A	E	I	N	S	T	TC NO 1 FRANÇAIS		
0	1	2	3	4	5	6			
B	C	D	F	G	H	J	K	L	M
70	71	72	73	74	75	76	77	78	79
O	P	Q	R	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	( )	(+)	(-)	(=)	REQ	ESP
90	91	92	93	94	95	96	97	98	99

```
TABLE DE CONVERSION NO.1

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

German
(memorized by the keyword ANREIS)

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

```
UMRECHNUNGSTABELLE NO.1

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

Spanish
(memorized by the keyword SENORA)

CODE	A	E	N	O	R	S	TC NO 1 ESPAÑOL		
0	1	2	3	4	5	6			
B	C	D	F	G	H	I	J	K	L
70	71	72	73	74	75	76	77	78	79
M	P	Q	T	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	( )	(+)	(-)	(=)	REQ	ESP
90	91	92	93	94	95	96	97	98	99

```
TABLA DE CONVERCIÓN NO.1

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

Appendix B

Printable standard conversion table and codebook (English)

Memorised by the keyword ON A TIE

CONVERSION TABLE NO.1 (EN)

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

CODE TABLE NO.1

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 .....
208 COORDINATE	451 LOCATE	703 REPEAT	956 .....
217 COUNTRY	460 LOCATION	712 RESERVATION	965 .....
226 COVERT	479 MAIL	721 ROUTINE	974 .....
235 CURRENT	488 MEETING	730 SATELLITE	983 .....
244 DANGER	497 MESSAGE	749 SHIP	992 .....

Appendix C

Custom conversion table

(assign the most frequent characters in your language to digits 1 to 6)

CODE-0	-70	-80	FIG-90
-1	-71	-81	-91
-2	-72	-82	-92
-3	-73	-83	-93
-4	-74	-84	-94
-5	-75	-85	-95
-6	-76	-86	-96
	-77	-87	-97
	-78	-88	-98
	-79	-89	SPC-99

Custom codebook for 100 words or phrases

Three-digit codes with error detection
(each code differs at least two digits from any code)

000	253	505	758
019	262	514	767
028	271	523	776
037	280	532	785
046	299	541	794
055	307	550	802
064	316	569	811
073	325	578	820
082	334	587	839
091	343	596	848
109	352	604	857
118	361	613	866
127	370	622	875
136	389	631	884
145	398	640	893
154	406	659	901
163	415	668	910
172	424	677	929
181	433	686	938
190	442	695	947
208	451	703	956
217	460	712	965
226	479	721	974
235	488	730	983
244	497	749	992

When creating a custom codebook, make sure to use words, expression or phrases that are more efficient (use less digits) than the letters converted separately.

Appendix D

Custom codebook for 220 words or phrases

Four-digit codes with error detection
(each code differs at least two digits from any code and no transposition of neighbouring digits)

0000	0594	1582	2790	4675
0011	0660	1595	2882	4686
0022	0671	1661	2893	4697
0033	0682	1670	2992	4774
0044	0693	1683	3333	4785
0055	0770	1692	3342	4796
0066	0781	1771	3351	4884
0077	0792	1780	3360	4895
0088	0880	1793	3377	4994
0099	0891	1881	3386	5555
0110	0990	1890	3395	5564
0121	1111	1991	3443	5577
0132	1120	2222	3452	5586
0143	1133	2233	3461	5591
0154	1142	2240	3470	5665
0165	1155	2251	3487	5674
0176	1164	2266	3496	5687
0187	1177	2277	3553	5696
0198	1186	2284	3562	5775
0220	1199	2295	3571	5784
0231	1221	2332	3580	5797
0242	1230	2343	3597	5885
0253	1243	2350	3663	5894
0264	1252	2361	3672	5995
0275	1265	2376	3681	6666
0286	1274	2387	3690	6677
0297	1287	2394	3773	6684
0330	1296	2442	3782	6695
0341	1331	2453	3791	6776
0352	1340	2460	3883	6787
0363	1353	2471	3892	6794
0374	1362	2486	3993	6886
0385	1375	2497	4444	6897
0396	1384	2552	4455	6996
0440	1397	2563	4466	7777
0451	1441	2570	4477	7786
0462	1450	2581	4480	7795
0473	1463	2596	4491	7887
0484	1472	2662	4554	7896
0495	1485	2673	4565	7997
0550	1494	2680	4576	8888
0561	1551	2691	4587	8899
0572	1560	2772	4590	8998
0583	1573	2783	4664	9999

Appendix E

Pre-calculated sequence to create a custom codebook for 807 words or phrases

Four-digit codes with error detection
(each code differs at least two digits from any code and no transposition of neighbouring digits)

0000	0550	1166	1718	2305	2936	3521	4114	4681	5354	6038	6600	7231	7849	8583	9217	9933
0011	0564	1177	1732	2316	2949	3534	4123	4705	5367	6042	6611	7240	7854	8591	9229	9944
0022	0589	1188	1746	2324	2980	3545	4131	4737	5370	6050	6622	7256	7868	8601	9246	9955
0033	0605	1199	1769	2332	2992	3553	4140	4742	5402	6061	6633	7273	7876	8612	9258	9966
0044	0616	1202	1771	2347	3003	3568	4157	4756	5410	6074	6644	7282	7887	8630	9263	9977
0055	0624	1210	1780	2351	3014	3576	4162	4761	5421	6104	6655	7294	7903	8643	9274	9988
0066	0637	1221	1793	2360	3025	3587	4185	4774	5434	6116	6666	7315	7914	8654	9281	9999
0077	0648	1234	1808	2373	3031	3607	4203	4783	5445	6125	6677	7329	7926	8668	9295	
0088	0659	1245	1817	2406	3040	3618	4216	4809	5453	6132	6688	7337	7951	8675	9306	
0099	0660	1253	1829	2415	3056	3626	4224	4825	5468	6147	6699	7342	7965	8687	9327	
0102	0671	1267	1836	2423	3062	3632	4232	4858	5476	6151	6701	7350	7978	8696	9339	
0110	0682	1278	1860	2430	3089	3649	4247	4863	5487	6160	6712	7361	7997	8702	9348	
0121	0693	1286	1873	2442	3097	3651	4251	4884	5500	6173	6730	7374	8008	8710	9364	
0134	0708	1303	1881	2457	3105	3663	4260	4892	5511	6205	6748	7383	8017	8721	9371	
0145	0717	1314	1894	2461	3113	3674	4275	4915	5522	6213	6753	7396	8029	8734	9380	
0153	0729	1325	1909	2474	3124	3680	4302	4938	5533	6226	6776	7416	8036	8745	9392	
0167	0736	1331	1928	2489	3130	3695	4310	4959	5544	6237	6787	7438	8064	8759	9408	
0178	0762	1340	1952	2504	3141	3706	4321	4970	5555	6241	6795	7447	8070	8767	9436	
0186	0770	1356	1964	2513	3152	3719	4334	4994	5566	6252	6802	7452	8081	8778	9449	
0201	0781	1362	1975	2526	3169	3727	4345	5005	5577	6264	6810	7460	8093	8786	9485	
0212	0794	1389	1983	2537	3198	3738	4353	5016	5588	6270	6821	7479	8118	8800	9518	
0220	0807	1397	1991	2541	3204	3765	4368	5024	5599	6289	6834	7484	8127	8811	9559	
0235	0818	1404	2002	2552	3215	3773	4376	5032	5604	6309	6845	7491	8139	8822	9561	
0243	0839	1413	2010	2565	3223	3782	4387	5047	5613	6317	6857	7525	8146	8833	9573	
0254	0846	1426	2021	2570	3236	3790	4400	5051	5620	6320	6878	7532	8163	8844	9584	
0268	0861	1437	2034	2598	3242	3816	4411	5060	5639	6336	6886	7548	8171	8855	9596	
0276	0872	1441	2045	2603	3250	3828	4422	5073	5641	6343	6935	7557	8180	8866	9647	
0287	0880	1450	2053	2614	3261	3837	4433	5103	5652	6358	6954	7590	8192	8877	9653	
0304	0895	1465	2067	2625	3279	3859	4444	5115	5665	6372	6967	7602	8207	8888	9669	
0313	0919	1472	2078	2631	3300	3870	4455	5126	5678	6381	6982	7610	8228	8899	9676	
0326	0927	1498	2086	2640	3311	3883	4466	5137	5686	6394	6996	7621	8249	8904	9694	
0330	0956	1505	2101	2656	3322	3891	4477	5142	5697	6407	7007	7634	8265	8913	9704	
0341	0973	1516	2112	2662	3333	3908	4488	5150	5731	6418	7018	7645	8272	8925	9713	
0352	0984	1524	2120	2679	3344	3917	4499	5161	5740	6424	7039	7658	8284	8932	9720	
0365	0990	1530	2135	2709	3355	3929	4501	5174	5758	6431	7046	7667	8290	8941	9735	
0379	1001	1547	2143	2728	3366	3946	4512	5189	5764	6446	7063	7689	8338	8950	9741	
0398	1012	1551	2154	2763	3377	3960	4520	5206	5775	6459	7071	7700	8357	8976	9752	
0403	1020	1563	2168	2772	3388	3972	4535	5214	5792	6462	7080	7711	8369	8998	9768	
0414	1035	1579	2176	2784	3399	3985	4543	5225	5843	6475	7092	7722	8382	9009	9779	
0425	1043	1582	2187	2791	3401	3993	4554	5230	5856	6480	7109	7733	8395	9028	9805	
0432	1054	1606	2200	2819	3412	4004	4567	5248	5869	6493	7117	7744	8405	9037	9814	
0440	1068	1615	2211	2827	3420	4013	4578	5257	5885	6503	7128	7755	8419	9072	9823	
0451	1076	1623	2222	2838	3435	4026	4586	5262	5890	6514	7136	7766	8448	9083	9831	
0469	1087	1638	2233	2850	3443	4030	4608	5271	5963	6527	7164	7777	8456	9091	9840	
0497	1100	1642	2244	2864	3454	4041	4617	5283	5979	6540	7170	7788	8473	9107	9862	
0506	1111	1657	2255	2871	3467	4052	4629	5301	5981	6556	7181	7799	8494	9119	9889	
0515	1122	1661	2266	2882	3478	4065	4636	5312	5995	6569	7195	7801	8509	9138	9897	
0523	1133	1670	2277	2893	3486	4079	4650	5323	6006	6571	7208	7812	8558	9156	9900	
0531	1144	1684	2288	2907	3502	4098	4664	5335	6015	6585	7219	7820	8560	9182	9911	
0542	1155	1707	2299	2918	3510	4106	4672	5346	6023	6592	7227	7835	8574	9190	9922	

Appendix F

Digit-to-words table

DIGIT TO WORDS

-0--------	-1--------	-2--------	-3--------	-4--------	-5--------	-6--------	-7--------	-8--------	-9--------
ARM	ACCOUNT	AIRPORT	AFTERNOON	AIRPLANE	BAR	BACKPACK	APPARTMENT	AIR	BED
BLOUSE	AIRCO	BLACK	AIRCRAFT	BELT	BATHROOM	BATH	ATTIC	BANK	BIKE
CAR	BOAT	BOOTS	BOOK	CALENDER	BLUE	BEDROOM	BEACH	BIRD	BOY
CLOUD	BOTTLE	BUILDING	BROTHER	CELLAR	BUS	BEER	CIGAR	BRIDGE	CHIPS
DOG	E-MAIL	CHAIR	CAT	CHOCOLAT	CIGARETTE	BIRTHDAY	COLLEAGUE	COAST	COUCH
FLOWER	FEET	CHEESE	CD	FATHER	COFFEE	CLOSET	COMPUTER	COKE	FOG
FRUIT	FINGER	CITY	EAR	FUEL	DOCTOR	EVENING	CROSSING	DAUGHTER	FOOTBALL
GASOLINE	GAS	DAY	EYE	HAIR	FRIEND	FERRY	DOOR	FACTORY	HAND
GLASSES	HART	FUNERAL	FLOOR	HOLIDAY	GRAY	FIELD	FRIDAY	FAX	LAKE
HOME	HOUSE	GARAGE	FOOD	KITCHEN	HOT-DOG	FISH	HAMBURGER	FRIDGE	LIPS
HUSBAND	LIBRARY	GRASS	FREEZER	MOUNTAIN	MOBILE	GARDEN	HAT	FRIENDSHIP	MAGAZINE
POOL	MORNING	LETTER	GREEN	NEWSPAPER	MOTOR	HAMMER	KNEE	GIRL	PORT
PROGRAM	PICK-UP	MONDAY	HOTEL	NIGHT	MOUTH	HI-FI	LEG	HORSE	SAUNA
SEAT	RED	MOVIE	JACKET	PASTA	SEA	MANAGER	MUSIC	MONTH	SCREWDRIVER
STATION	SATURDAY	PANTS	MOTHER	PHONE	SOFA	MONEY	OFFICE	RADIO	SODA
TABLE	SHOES	POSTMAN	PETROL	SKIRT	STORE	SCARF	OIL	RUGBY	SOUND
TOAST	STREET	RAIN	POLICE	STORM	TUESDAY	SHIP	SANDWICH	SHIRT	SWEATER
TOWN	TREE	SHOP	RIVER	TEACHER	TV	STOMACH	SON	SNOW	TEA
VIDEO	VEGETABLES	SOCKS	ROAD	TODAY	VEST	SUN	TOMORROW	STAIRS	THURSDAY
WEDDING	WIFE	TOOL	STEREO	TOILET	WEATHER	SUNDAY	TRAIN	STEAK	TUNNEL
WEDSNESDAY	WINDOW	TRUCK	SISTER	TRAFFIC	WEEK	VILLAGE	WIND	SUBWAY	WEEKEND
YESTERDAY	WRENCH	WINE	TENNIS	VAN	WHISKEY	WATER	YELLOW	YEAR	WHITE

WORD TO DIGIT

1 ACCOUNT	7 CIGAR	1 GAS	7 OFFICE	8 SUBWAY
3 AFTERNOON	5 CIGARETTE	0 GASOLINE	7 OIL	6 SUN
8 AIR	2 CITY	8 GIRL	2 PANTS	6 SUNDAY
1 AIRCO	6 CLOSET	0 GLASSES	4 PASTA	3 SISTER
3 AIRCRAFT	0 CLOUD	2 GRASS	3 PETROL	9 SWEATER
4 AIRPLANE	8 COAST	5 GRAY	4 PHONE	0 TABLE
2 AIRPORT	5 COFFEE	3 GREEN	1 PICK-UP	9 TEA
7 APPARTMENT	8 COKE	4 HAIR	3 POLIC	4 TEACHER
0 ARM	7 COLLEAGUE	7 HAMBURGER	0 POOL	3 TENNIS
7 ATTIC	7 COMPUTER	6 HAMMER	9 PORT	9 THURSDAY
6 BACKPACK	9 COUCH	9 HAND	2 POSTMAN	0 TOAST
8 BANK	7 CROSSING	1 HART	0 PROGRAM	4 TODAY
5 BAR	8 DAUGHTER	7 HAT	8 RADIO	4 TOILET
6 BATH	2 DAY	6 HI-FI	2 RAIN	7 TOMORROW
5 BATHROOM	5 DOCTOR	4 HOLIDAY	1 RED	2 TOOL
7 BEACH	0 DOG	0 HOME	3 RIVER	0 TOWN
9 BED	7 DOOR	8 HORSE	3 ROAD	4 TRAFFIC
6 BEDROOM	3 EAR	5 HOT-DOG	8 RUGBY	7 TRAIN
6 BEER	1 E-MAIL	3 HOTEL	7 SANDWICH	1 TREE
4 BELT	6 EVENING	1 HOUSE	1 SATURDAY	2 TRUCK
9 BIKE	3 EYE	0 HUSBAND	9 SAUNA	5 TUESDAY
8 BIRD	8 FACTORY	3 JACKET	6 SCARF	9 TUNNEL
6 BIRTHDAY	4 FATHER	4 KITCHEN	9 SCREWDRIVER	5 TV
2 BLACK	8 FAX	7 KNEE	5 SEA	4 VAN
0 BLOUSE	1 FEET	9 LAKE	0 SEAT	1 VEGETABLE
5 BLUE	6 FERRY	7 LEG	6 SHIP	5 VEST
1 BOAT	6 FIELD	2 LETTER	8 SHIRT	0 VIDEO
3 BOOK	1 FINGER	1 LIBRARY	1 SHOE	6 VILLAGE
2 BOOT	6 FISH	9 LIPS	2 SHOP	6 WATER
1 BOTTLE	3 FLOOR	9 MAGAZINE	4 SKIRT	5 WEATHER
9 BOY	0 FLOWER	6 MANAGER	8 SNOW	0 WEDDING
8 BRIDGE	9 FOG	5 MOBILE	2 SOCK	0 WEDSNESDAY
3 BROTHER	3 FOOD	2 MONDAY	9 SODA	5 WEEK
2 BUILDING	9 FOOTBALL	6 MONEY	5 SOFA	9 WEEKEND
5 BUS	3 FREEZER	8 MONTH	7 SON	5 WHISKEY
4 CALENDER	7 FRIDAY	1 MORNING	9 SOUND	9 WHITE
0 CAR	8 FRIDGE	3 MOTHER	8 STAIRS	1 WIFE
3 CAT	5 FRIEND	5 MOTOR	0 STATION	7 WIND
3 CD	8 FRIENDSHIP	4 MOUNTAIN	8 STEAK	1 WINDOW
4 CELLAR	0 FRUIT	5 MOUTH	3 STEREO	2 WINE
2 CHAIR	4 FUEL	2 MOVIE	6 STOMACH	1 WRENCH
2 CHEESE	2 FUNERAL	7 MUSIC	5 STORE	8 YEAR
9 CHIPS	2 GARAGE	4 NEWSPAPER	4 STORM	7 YELLOW
4 CHOCOLAT	6 GARDEN	4 NIGHT	1 STREET	0 YESTERDAY

Appendix G

Morse Cut Numbers

Various cut numbers systems to shorten the transmission time of Morse digits

Morse Full Numbers		Morse Cut Numbers									
		Standard Short		International		CIS 1		CIS 2		Cuban	
1	·----	1	·- (A)	1	·- (A)	1	·- (A)	1	·- (A)	1	·- (A)
2	··---	2	··- (U)	2	··- (U)	2	···· (B)	2	·-- (W)	2	·· (N)
3	···--	3	···- (V)	3	·-- (W)	3	·-- (W)	3	· (E)	3	··· (D)
4	····-	4	····- (4)	4	···- (V)	4	-·· (G)	4	·-· (R)	4	···- (U)
5	·····	5	· (E)	5	··· (S)	5	-·· (D)	5	- (T)	5	·-- (W)
6	-····	6	-···· (6)	6	-··· (B)	6	· (E)	6	-··- (Y)	6	·-· (R)
7	--···	7	-··· (B)	7	--· (G)	7	···- (V)	7	··- (U)	7	·· (I)
8	---··	8	-·· (D)	8	-·· (D)	8	-···· (Z)	8	·· (I)	8	-·· (G)
9	----·	9	-· (N)	9	-· (N)	9	·· (I)	9	--- (O)	9	-- (M)
0	-----	0	- (T)	0	- (T)	0	-·- (K)	0	·--· (P)	0	- (T)