The Two Time Pad Encryption System

This document describe the use and function of a one-time-pad style encryption system for field and educational use. You may download sheets free from www.randomserver.dyndns.org/client/random.php to play with, or use to protect personal secret communication.

Introduction

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

How the encryption works

In the classic one-time-pad[i], the plaintext letters are added to a key by addition. A typical implementation is to convert the plaintext into numerical form, and then encrypt the plaintext numbers by adding a secret numerical key. Instead, this implementation use random substitution alphabets as the key. To make decoding easier, the substitution is reciprocal, so if the letter A encrypts to W, the letter W will encrypt back to an A. A substitution alphabet is much stronger compared to a simple addition of letters, so each alphabet can be used for several letters before there is a risk that the code can be broken[ii].

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

[i] First known description: Miller, Frank (1882). *Telegraphic code to insure privacy and secrecy in the transmission of telegrams.* C.M. Cornwell.
[ii] see security analysis
[iii] historical sources mention this problem occasionally.
see Benson, Robert L.. "The Venona Story". National Security Agency.

How to set up a network

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

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

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

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

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

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

[iv] an example sheet is at the end of this document

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

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

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

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

An alternative method would be to download several series right now, using the computer of a friend or an office, and then use this only later, if needed. Even if a security agency hold a copy of the tables, it could be problematic to identify the download a year later.

Security Analysis

The max entropy of a letter is log(48)/log(2) = 5.58 bits, as there are 48 chars in the alphabet. The entropy of a alphabet is log(W)/log(2); W=48*46*44*42*40*38*...*8*6*4*2=(all possible combinations)=10.4E30=2^103;

[v] http://www.randomserver.dyndns.org/client/random.php

[vi] if you incinerate the pages in your hotel room smoke or fire alarms might be an issue

[vii] China, USA, (and France and possibly even Germany ...)

[viii] this refer to that the espionage is intended and used for commercial purposes

[ix] a friend reported while working with Police in Philippines, he had a kind of police-scanner that monitored and decoded cell phone traffic (personal communication)

[x] best is to re-install the operating system and printer drivers using only CD:s. No internet connection at any time for any purpose. Block WiFi if present.

or 103 bits of entropy in each alphabet. For "perfect" security[xi] this key will last for 103/5.58=18.4 characters, and if we include approx 1 bit of entropy for each plaintext character, no unique decoding[xii] will be possible for 103/(5.58-1)=22 chars. Using each alphabet for two times 4 characters seems to be safe.
If each table is used for two encryptions (double use) and one message becomes completely known to the analyst, identical or reciprocal characters at identical positions will be known. Likely a guess can be made also at other characters. Likely, decoding the unknown message could prove difficult.

Document Revision History

2012-02-14 Initial version.
2012-03-23 Update, small changes.

[xi] the key is rich enough to be able to decode an intercepted ciphertext into ANY plaintext message
[xii] the key is rich enough to be able to decode an intercepted ciphertext into several/many possible plaintext messages

```
P: HELLO+BILL+THIS+IS+
C: J6*U5K3JZ*2G#JVK#;%
Printing encryption sheets #1 to #1

      ---  ---  ---  ---   ---  ---  ---  ---   ---  ---
Group:    1
                                                XXX
P1:   _H_  _E_  _L_  _L_   _O_  _+_  _B_  _I_   XXX  _L_
                                                XXX
C1:   _J_  _6_  _*_  _U_   _5_  _K_  _3_  _J_   XXX  _Z_
       |    |    |    |     |    |    |    |     |    |
      XXX  XXX                  XXX
P2:   XXX  XXX  _L_  _+_   _T_  XXX  _H_  _I_   _S_  _+_
      XXX  XXX                  XXX
C2:   XXX  XXX  _*_  _2_   _G_  XXX  _#_  _J_   _V_  _K_
       |    |    |    |     |    |    |    |     |    |
                     XXX             XXX
P3:   _I_  _S_  _+_  XXX   ___  ___  XXX  ___   ___  ___
                     XXX             XXX
C3:   _#_  _;_  _%_  XXX   ___  ___  XXX  ___   ___  ___
       |    |    |    |     |    |    |    |     |    |
                XXX             XXX       XXX
P4:   ___  ___  XXX  ___   ___  XXX  ___  XXX   ___  ___
                XXX             XXX       XXX
C4:   ___  ___  XXX  ___   ___  XXX  ___  XXX   ___  ___
       |    |    |    |     |    |    |    |     |    |
                           XXX                       XXX
P5:   ___  ___  ___  ___   XXX  ___  ___  ___   ___  XXX
                           XXX                       XXX
C5:   ___  ___  ___  ___   XXX  ___  ___  ___   ___  XXX
       |    |    |    |     |    |    |    |     |    |
      0 D  0 %  0 4  0 =   0 5  0 "  0 /  0 K   0 U  0 4
      1 #  1 G  1 S  1 K   1 /  1 2  1 R  1 J   1 =  1 B
      2 X  2 J  2 ;  2 +   2 "  2 I  2 8  2 P   2 ;  2 #
      3 "  3 =  3 3  3 "   3 -  3 #  3 B  3 3   3 9  3 *
      4 Z  4 V  4 O  4 %   4 L  4 4  4 Q  4 A   4 N  4 O
      5 +  5 7  5 5  5 H   5 O  5 Z  5 7  5 6   5 +  5 7
      6 N  6 E  6 Y  6 M   6 W  6 M  6 X  6 5   6 G  6 W
      7 P  7 5  7 K  7 G   7 U  7 E  7 5  7 -   7 8  7 5
      8 Y  8 M  8 E  8 T   8 B  8 ?  8 2  8 8   8 7  8 U
      9 G  9 9  9 M  9 S   9 X  9 ;  9 L  9 "   9 3  9 =
      - E  - .  - =  - *   - 3  - D  - G  - 7   - B  - ?
      A .  A X  A D  A V   A Q  A U  A ?  A 4   A ?  A C
      B U  B T  B R  B B   B 8  B @  B 3  B F   B -  B I
      C S  C Z  C X  C Z   C Z  C V  C =  C .   C P  C A
      D O  D U  D A  D E   D N  D -  D @  D R   D J  D S
      E -  E 6  E 8  E D   E F  E 7  E M  E =   E Q  E J
      F L  F ?  F H  F .   F E  F N  F .  F B   F #  F T
      G 9  G I  G "  G 7   G T  G L  G -  G Z   G 6  G .
      H J  H L  H F  H 5   H #  H H  H #  H U   H /  H R
      I #  I G  I S  I K   I /  I 2  I R  I J   I =  I B
      J H  J 2  J W  J #   J *  J P  J S  J I   J D  J E
      K ?  K N  K 7  K I   K Y  K +  K %  K O   K R  K +
      L F  L H  L *  L U   L 4  L G  L 9  L Y   L X  L Z
      M /  M 8  M 9  M 6   M S  M 6  M E  M T   M W  M @
      N 6  N K  N @  N Y   N D  N F  N P  N %   N 4  N %
      O D  O %  O 4  O =   O 5  O "  O /  O K   O U  O 4
      P 7  P "  P T  P ?   P ;  P J  P N  P 2   P C  P ;
      Q W  Q /  Q V  Q Q   Q A  Q W  Q 4  Q @   Q E  Q "
      R @  R W  R B  R @   R %  R /  R I  R D   R K  R H
      S C  S ;  S I  S 9   S M  S .  S J  S V   S V  S D
      T ;  T B  T P  T 8   T G  T *  T T  T M   T *  T F
      U B  U D  U ?  U L   U 7  U A  U Z  U H   U O  U 8
      V =  V 4  V Q  V A   V @  V C  V Y  V S   V S  V X
      W Q  W R  W J  W X   W 6  W Q  W W  W +   W M  W 6
      X 2  X A  X C  X W   X 9  X Y  X 6  X /   X L  X V
      Y 8  Y #  Y 6  Y N   Y K  Y X  Y V  Y L   Y "  Y /
      Z 4  Z C  Z .  Z C   Z C  Z 5  Z U  Z G   Z @  Z L
      . A  . -  . Z  . F   . ?  . S  . F  . C   . %  . G
      + 5  + +  + %  + 2   + =  + K  + ;  + W   + 5  + K
      ; T  ; S  ; 2  ; /   ; P  ; 9  ; +  ; ?   ; 2  ; P
      = V  = 3  = -  = O   = +  = %  = C  = E   = I  = 9
      / M  / Q  / #  / ;   / I  / R  / O  / X   / H  / Y
      * %  * @  * L  * -   * J  * T  * "  * #   * T  * 3
      % *  % O  % +  % 4   % R  % =  % K  % N   % .  % N
      # I  # Y  # /  # J   # H  # 3  # H  # *   # F  # 2
      @ R  @ *  @ N  @ R   @ V  @ B  @ D  @ Q   @ Z  @ M
      " 3  " P  " G  " 3   " 2  " O  " *  " 9   " Y  " Q
      ? K  ? F  ? U  ? P   ? .  ? 8  ? A  ? ;   ? A  ? -
```