CIPHER MACHINES AND CRYPTOLOGY

Straddling Checkerboards

Home One-time pad

This page contains some examples of straddling checkerboards, a system to encode plain text into digits. This encoding is not a type of encryption and offers absolutely no cryptographic security whatsoever! The encoding only prepares the plaintext for the actual encryption process. Therefore, we call the result of encoding a plaincode, to stress that the message is still in its plain readable form.

These checkerboards are easily designed from scratch or customized to fit the requirements of its users. This can range from simple text-only encoding to the use of special characters, words or codes for specific purposes or languages. The presented examples show the basic properties and possibilities of the checkerboard text-to-digit encoding. Anything is possible, as long as both sender and receiver agree upon a common system. The straddling checkerboard encodes the most frequently used letters into one-digit values. All other letters are encoded into two-digit values. This reduces the size of the message considerably (approx 1.5 digit/letter ratio against 2.0 for fixed two-digit systems).

A checkerboard also breaks up individual letters into seperate parts. This is called fractionation. Moreover, it does this irregularly (some are single and some double-digit values). When the checkerboard encoding is followed by an encryption algorithm that transposes the plaincode digits, then the irregular fractionation will cause the characters to be torn apart in a most irregular fashion and produce a far more complex encryption. Often, such encryption methods also use a checkerboard that has the order of its letters or digits scrambled to increase the total strength of the encryption.

Note that the fractionation properties and scrambled letters or digits are irrelevant when the checkerboard encoding is followed by one-time pad encryption, as this type of encryption is unbreakable anyway. Here, only the checkerboard's efficiency matters. Please visit the one-time pad page for more information about the use of checkerboards for one-time pad encryption.

Some Checkerboard Variations

A basic checkerboard, letter-optimised for English and based on the "AT ONE SIR" mnemonic, a table easily composed and wirtten out on paper.

	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	/

The table speaks for itself. "F/L" (68) is used to switch to figures and back to letters. Numbers are usually written out three times to exclude errors. The text "A54H" will therefore encode into "0 68 555 444 68 25". The field "/" (69) is used to seperate letters or sentences. We can change the order of the top row letters to any desired combination. Some other anagram arragements for the "AT-ONE-SIR" top row letters are "SENORITA--" are "A-NOTE-SIR", "NATO-RISE-", "RAT-NOISE-", or "NO-TEA-SIR". If we change the position of the two blank fields in the top row, then we also need to replace the digit labels for the second and third row with the digits that correspond to the top row empty cells. We can also replace the top row letters by to the most frequently used letters of another language. These can vary quite a bit depending on the language. For more details, visit the letter frequency wiki page.

Let's give a short example of how the checkerboard works by encoding the text "CONTACT JOHN AT 1830H". The top row letters are encoded into a single-digit value by taking the digit above the letter. The other letters are encoded in a two-digit value by taking the row digit, followed by the column digit. Once encoded into digits, we can encrypt the message with any digits based encryption algorithm.

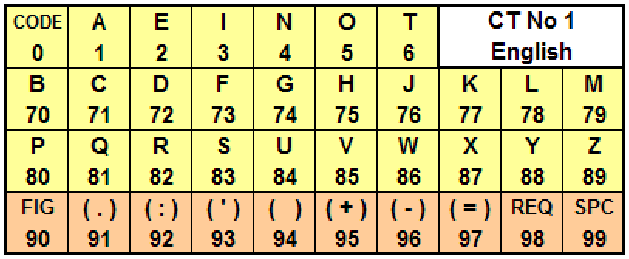
```
Plaintext:  C  O  N  T  A  C  T   J  O  H  N    A  T  [fig]  1   8   3   0  [ltr] H
Plaincode:  21 3  4  1  0  21 1   26 3  25 4    0  1   68   111 888 333 000  68   25

In groups:  21341 02112 63254 01681 11888 33300 06825
```

When decoding the message back from digits into text, we can easily distinguish single-digit from double-digit combinations. If the first next digit represents a letter in the top row, we have a single-digit value and simply take the letter underneath that digit. If however the digit is located on the left-hand side of a row then we have encoutered the first part of a double-digit value and must take the intersection of that digit's row and the following digit's column to find the letter that corresponds to that double-digit value.

Although the checkerboard from above is simple to compose and to use, you can format such a table in another more practical and faster format for complex checkerboards with a larger number of cells:

A 0	T 1	 2	O 3	N 4	E 5	 6	S 7	I 8	R 9
B 20	C 21	D 22	F 23	G 24	H 25	J 26	K 27	L 28	M 29
P 60	Q 61	U 62	V 63	W 64	X 65	Y 66	Z 67	L/F 68	/ 69

The following standard checkerboard is also optimised for English and has some extre features. Note that each additional empty cell in the top row enables the creation of an additional row with 10 new characters.

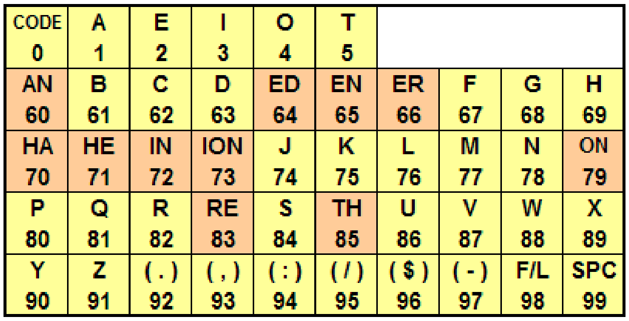


CODE 0	A 1	E 2	I 3	N 4	O 5	T 6	CT No 1 English		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	S 83	U 84	V 85	W 86	X 87	Y 88	Z 89
FIG 90	(.) 91	(:) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	SPC 99

This checkerboard incorporates several puntuation and the space "SPC" (99). Here, "FIG" (90) has the same function as the "L/F" field from the previous table. The "REQ" (98) field is the abbreviation of "REQUEST" as in "request help" or "request new supplies". The table also contains a "CODE" field. This "CODE" prefix is used in combination with an additional codebook. Such codebooks contain all kinds of words, expressions or standard sentences, represented by a three-figure or four-figure code, depending on the codebook that is used. If, for example, "245" represents "Request more information" in the codebook, this would be encoded into "0245". Always use the "CODE" prefix (in this example "0") as prefix just before the actual code. When the receiver encounters the "CODE" prefix, he knows that he must decode the following three digits with the proper codebook into a word or phrase. The use of a codebook is optional but can reduce the message length considerably.

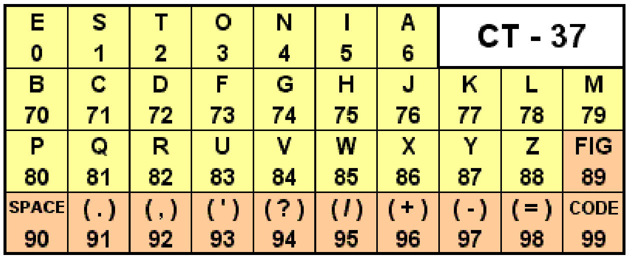
The top row with most frequently used English letters for this checkerboard is memorised by the words "ON A TIE" in alphabetic order. We can optimise this checkerboard for French by using, in alphabetic order, the letters from the word "SAINTE". For German this would be "ANREIS "and for Spanish "SENORA". This, of course, requires a different completion of the second and third row with the remaining letters.

The following checkerboard, also optimised for English, includes the most common English digraphs. This again reduces the required digits for certain words.



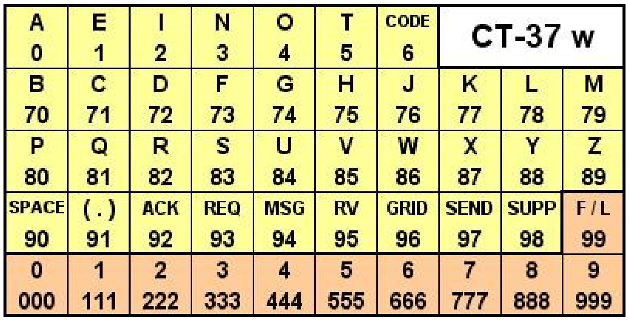
CODE 0	A 1	E 2	I 3	O 4	T 5				
AN 60	B 61	C 62	D 63	ED 64	EN 65	ER 66	F 67	G 68	H 69
HA 70	HE 71	IN 72	ION 73	J 74	K 75	L 76	M 77	N 78	ON 79
P 80	Q 81	R 82	RE 83	S 84	TH 85	U 86	V 87	W 88	X 89
Y 90	Z 91	(.) 92	(,) 93	(:) 94	(/) 95	($) 96	(-) 97	F/L 98	SPC 99

The CT-37 table is another extended version of the straddling checkerboard that includes additional characters. The table is easy to remember. It uses the 7 most frequent English letters "ESTONIA" in the top row. The two following rows are the remaining letters, completed with the "FIG" (89) field. The fourth row contains the "SPACE" (90) and "CODE" (99) field with the punctuation marks between them (less critical to remember).



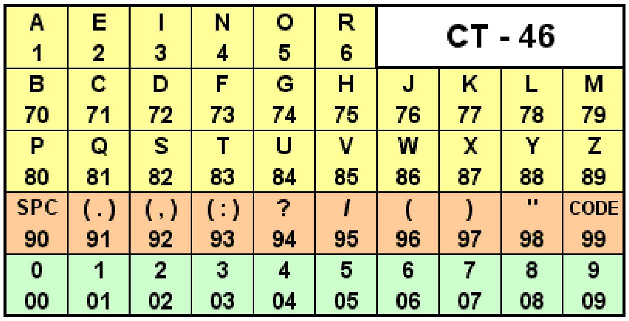
E 0	S 1	T 2	O 3	N 4	I 5	A 6	CT - 37		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	U 83	V 84	W 85	X 86	Y 87	Z 88	FIG 89
SPACE 90	(.) 91	(,) 92	(') 93	(?) 94	(/) 95	(+) 96	(-) 97	(=) 98	CODE 99

The CT-37-Words table uses a mix of letters, words and code. "CODE" (6) is a shortened prefix for fixed length codes. The commonly used words "acknowledge", "request", "message", "rendez-vous point", "grid" (coordinates), "send" and "supply" are respresented by a small two-digit code. Omitting one more top-row letter or the CODE field will give another full row which could held 10 more words, expressions or short sentences (CODE could be added to this new row). This approach can reduce the message length enormously if the set of two-digit expressions is selected carfully.



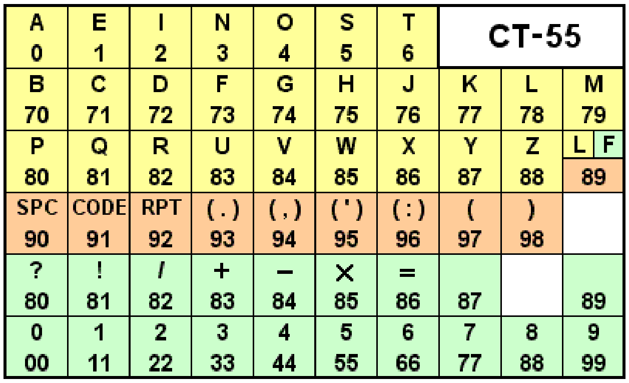
A 0	E 1	I 2	N 3	O 4	T 5	CODE 6	CT-37 w		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	S 83	U 84	V 85	W 86	X 87	Y 88	Z 89
SPACE 90	(.) 91	ACK 92	REQ 93	MSG 94	RV 95	GRID 96	SEND 97	SUPP 98	F / L 99
0 000	1 111	2 222	3 333	4 444	5 555	6 666	7 777	8 888	9 999

In the CT-46 encoding table, we can use four full rows since we have four unused digits in the top row. This encoding table is not that hard to memorize. In the first row the 6 most frequent letters AEINOR get the single digits. Each next row starts with the remaining digits 7, 8, 9 or 0. The second and third row are the remaining letters of the alphabet. The fourth row contains the "SPC"(90) and "CODE" (99) with the signs in between (less important to memorize). The fifth row are simply the numbers preceded by a zero.



A	E	I	N	O	R	CT - 46			
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	S	T	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
SPC	(.)	(,)	(:)	?	/	(	)	"	CODE
90	91	92	93	94	95	96	97	98	99
0	1	2	3	4	5	6	7	8	9
00	01	02	03	04	05	06	07	08	09

The CT-55 table has even more additional characters. "L/F" (89) is used to switch from Letters (yellow) to Figures (green) and from Figures to Letters. This enables more characters with the same encoding value. The Red fields can be used in both Letters and Figures mode, thus a space, period, etc in a text doesn't require switching to Figures. Numbers are represented by its double code to exclude digit errors. An example: "F-16B" is encoded into 73 89 84 11 66 89 70. "CODE" (91) is again used as a prefix for four-digit codes and "RPT" (92) is used to repeat important pieces of text. This encoding table has the 7 most frequent letters, optimized for English, and is suitable for text with more figures and signs.



A	E	I	N	O	S	T	CT-55		
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	U	V	W	X	Y	Z	L F
80	81	82	83	84	85	86	87	88	89
SPC	CODE	RPT	(.)	(,)	(')	(:)	(	)	
90	91	92	93	94	95	96	97	98	
?	!	/	+	−	×	=			
80	81	82	83	84	85	86	87		89
0	1	2	3	4	5	6	7	8	9
00	11	22	33	44	55	66	77	88	99

Of course, there are many other ways to encode characters into digits. The system of encoding characters into digits doesn't need to be scrambled or secure in any way when one-time pad encryption provides the security. Any method to encode into digits is good, as long as it is practical, doesn't make the message too long and isn't prone to critical errors. The shown examples are easily adapted to anyone's specific purposes.

Scrambled Checkerboards

As explained before, checkerboards that are used in combination with an encryption method, other than one-time pad, preferably contain a scrambled alphabet or digits. This will strengthen the subsequent encryption considerably. Note that there are far more possible ways to scramble the alphabet than to scramble 10 digits. Therefore, we will focus on creating keyword based scrambled alphabets that include optimised letter frequency for a given language.

Our first example uses two keywords and a double transposition. Let's use the keywords "OVERTURE" and "INTERGALACTIC". A first matrix is created with the first keyword and filled with the normal alphabet. A second, for now empty matrix, is created with the second keyword. The letters of both keywords are numbered according to their order in the alphabet. Doe letters that occure more than once we assign the lowest number to the most-left letter.

Read off the letters of the first matrix, column by column, as determined by the first keyword order, and fill the second matrix, row by row, with those letters.

```
  O V E R T U R E   I  N  T  E  R  G  A  L  A  C  T  I  C
  3 8 1 4 6 7 5 2   7  10 12 5  11 6  1  9  2  3  13 8  4
  ---------------   -------------------------------------
  A B C D E F G H   C  K  S  H  P  X  A  I  Q  Y  D  L  T
  I J K L M N O P   G  O  W  E  M  U  F  N  V  B  J  R  Z
  Q R S T U V W X
  Y Z
```

Next, read off and write down the letters from the second matrix, column by column, in the order as determined by the second keyword, and mark all most-frequent English letters, as provided by the mnemonic "AT ONE SIR".

```
  AF QV YB TZ HE XU CG LR IN KO PM SW DJ
  x        x   x        x xx  x    x
```

Finally, the checkerboard is filled with the scrambled letters, the marked most-frequent letters in the top row, followed by the remaining letters. If we use the "AT-ONE-SIR" checkerboard from the first example on this page, the result is as follows:

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

The second example uses two keywords and a single transposition. Let's again take the keywords "OVERTURE" and "INTERGALACTIC". Write out the letters of the first keyword and number them according to their order in the alphabet. Also here, letters that occure more than once have the lowest number assigned to the most-left letter. Next, the matrix is filled with the second key word, without repeating any of the letters from that keyword. Complete the matrix with the remaining letters of the alphabet.

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

Read off the letters in the matrix, column by column, in the order as determined by the first keyword and mark all most-frequent English letters "AT ONE SIR".

```
TDQ LMX ICOY EFS AKW RHU GJV NBPZ
x       x x  x x x  x       x
```

Finally, the checkerboard is filled with the marked frequent letters first, followed by the remaining letter in the "AT-ONE-SIR" checkerboard:

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

Notice the completely different alphabets, created with the same two keywords but another transposition method. Although both methods create an excellent mix, it should be noted that the double transposition with two matrices creates the superior mix. Of course, these scrambled alphabets are useable for various differently formatted checkerboard and we could even fill the matrices with a mix of letters, digits, codes or punctuations.

On its own, these scrambled checkerboards constitue a monoalphabetic cipher, somewhat complicated by the irregular fractionation of the single and double digit combinations. This however will not provide any serious protection agains basic cryptalanysis, even by a novice codebreaker. It's real potential is only fully exploited when a text, encoded with a scrambled checkerboard, is followed by a double transposition of the plaincode digits. A final increase of complexity is achieved if one or both of the these transpositions are disrupted. This combination creates one of the most powerfull manual cipher system that exist. This is due to the suppression of high frequency letters in combination with the highly irregular fractionation of the digit combinations by the two transpositions. Note that the matrices of this subcequent duoble transposition should preferably be unequal in width, one of even and one of odd width, and at least 15 to 20 columns wide. Remember, it's not required to scrambled a checkerboard when the encoded message is followed by one-time pad encryption, as this type of encryption provides absolute security on its own.

Additional information

- One-time pad History and description of one-time pad encryption
- Guide to Secure Communications with the One-time Pad Cipher how to use one-time pads, text-to-digit encoding systems and codebooks
- SAS und Chiffrierdienst website contains many different encoding tables and manual encryption methods, used by Intelligence agencies.
- Letterfrequency.org Various letter and word frequencies in different languages, useful to optimize checkerboards
- CT-46 OTP One Time Pad Training Tool (direct Zip download)

Home One-time pad