Description of Sturgeon (T52a/b model) cipher machine

Introduction

The T52a/b is a German teleprinter and a cipher machine. It emits or receive characters. If the Cipher mode is set, each character is ciphered before it is emitted or deciphered before is is received. If the sender and receiver have set their machine on the same way (they uses the same key), they exchange texts in clear text from their point of view. An other people who taps the dialogue views only gibberish (the cipher text).

Teleprinter

A teleprinter uses the Baudot code. This one codes letters, figures and some others characters ('+', '/', ...) with five bits for each character. Each five bits configuration correspond to two characters. The good interpretation is function of the present mode: letter or figure one. For exemple, in letter mode, the bits string 10000 means letter 'E', but it means the number '3' in the figure mode.

The are special characters with special meaning
(but with the same meaning in letter and figure mode):

00010	CR	(Carriage Return)
01000	NL	(New Line)
11111	LS	(Letter Switch: switchs from figure mode to letter mode)
11011	FS	(Figure Switch: switchs from to letter mode to figure mode)
00100	SP	(Space)
00000	BL	(Blank: Empty character)

Baudot Code

```
Letter mode (with Bletchley representation of the special characters)
    '/':'00000', 'E':'10000', '4':'01000', '9':'00100', '3':'00010',
    'T':'00001', 'A':'11000', 'S':'10100', 'D':'10010', 'Z':'10001',
    'I':'01100', 'R':'01010', 'L':'01001', 'N':'00110', 'H':'00101',
    'O':'00011', 'U':'11100', 'J':'11010', 'W':'11001', 'F':'10110',
    'Y':'10101', 'B':'10011', 'C':'01110', 'P':'01101', 'G':'01011',
    'M':'00111', 'K':'11110', 'Q':'11101', '+':'11011', 'X':'10111',
    'V':'01111', '8':'11111'
Figure mode
    '#':'00000', '3':'10000', '#':'01000', '#':'00100', '#':'00010',
    '5':'00001', '-':'11000', "'":'10100', '#':'10010', '+':'10001',
    '8':'01100', '4':'01010', ')':'01001', ',':'00110', '*':'00101',
    '9':'00011', '7':'11100', '#':'11010', '2':'11001', '*':'10110',
    '6':'10101', '?':'10011', ':':'01110', '0':'01101', '*':'01011',
    '.':'00111', '(':'11110', '1':'11101', '#':'11011', '/':'10111',
    '=':'01111', '@':'11111'
}
```

Remarks: Berkeley codification uses only the text part with a spcial representations of special characters (CR, LF, LS, FS, SP, BL).

Example of sentence:
- In German: "ES IST DER 4. FEBRUAR 1942 [LF] [CR]“
- In Baudot code (Bletchley representation): ES9IST9DER9+RM98FEBRUAR9+QORW43

Cipher mode – introduction

The bits of each character undergo an addition without carry (XOR) and a permutation.

Example:
- Plain character: 01001 (L)
- Addition character: 01110
- Result: 00111
- Permutation: 53241
- Crypto character: 11010 (J)

The addition character and the permutation change at each step (at each character). The Permutation is based on a electric circtuit built from the internal key. It consists of five permutations. A key character actives or does not actives each of theses five permutations. The permutation takes place if the correspond bit is zero.

Example
- Permutation circuit: (1-5), (4-5), (3-4), (2-3), (1-2) [bit 1 is exchanged (or not) with bit 5, ...]
- Permutation character: 01101
- Effective permutation: (1-5), -, -, (2-3), - : 53241

Cipher mode – generation of the bits stream

The ten bits keys (The Addition character and the Permutation character) come from ten wheels. They are named A from K (from right to left). At each step (at each character ciphered or deciphered), sensors read bits from the wheels and each wheel steps one sector. The wheels have a number of sectors first between them. As a result, we return to the starting position after several billion characters entered. Happily, the bit setting of each wheel is immutable (unlike the SZ40 cipher attachment).

```
Bit configuration of each wheel
            1         2         3         4         5         6         7
   12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345
K="0101110010101110011101111000111010000111110001 0"
J="0011100011100101110100001111000101101011011001 1010110"
H="1111000110100011010110001111110011010110100111110001111 0100"
G="1111010010011101011010110100001101001011101111000110011000101"
F="1011011110110011100001000011101111110001010101011111000010111100"
E="1111100101001101000010111110011101010110001010001000101111111 0101"
D="0001001110011100101110001100100101111001000101101010001110000011010"
C="0100001111011101110001001001110000110000110001011111010110011011000011"
B="0110111110000011100011011100000110101011100000101111001111110001000 1010"
A="0111010101110011001110110000011100011110100000010110111000100110010011110"
   12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345
```

Remark: For each Wheel, the sensor is before the benchmark which indicate the position of the wheel: K: 16 steps before position, J: 18 steps, H and G: 20 steps, F and E: 22 steps, D and C: 23 steps, B: 24 steps, A: 25 steps.

Exemple of bits stream for four characters ciphered (Position and sensor between parenthesis):

K	J	H	G	F	E	D	C	B	A	10 Bits
06(37)	16(51)	25(05)	31(11)	46(24)	36(14)	41(18)	06(52)	01(48)	09(57)	0 1 0 0 0 1 0 1 0 0
07(38)	17(52)	26(06)	32(12)	47(25)	37(15)	42(19)	07(53)	02(49)	10(58)	1 1 0 1 0 0 1 0 1 0
08(39)	18(53)	27(07)	33(13)	48(26)	38(16)	43(20)	08(54)	03(50)	11(59)	1 0 0 1 0 1 1 1 1 1
09(40)	19(01)	28(08)	34(14)	49(27)	39(17)	44(21)	09(55)	04(51)	12(60)	1 0 1 1 1 0 1 0 1 0

etc.

Inner-Key

The Inner key is the setting of the plugs that connect the wheels to the addition and permutation systems. Each wheel is associated with two plugs. Each plug is set in one of the 20 existing sockets. The sockets that configure the addition system are named Ia, Ib, IIa, IIb, IIIa, IIIb, IVa, IVb, Va, Vb. The names I, II, III, IV and V correspond to the five bits of the character configuring the addition (XOR). If the H Wheel configures the 2nd bit of the addition character, its two plugs must be put in sockets IIa and IIb. The sockets that configure the permutation system are named from 1 to 10. Each can receive one of the remaining plugs. Thus the black plug of the wheel F can be put in the socket 3 and the red plug of the wheel F put in the socket 8.

Example of an Inner-key:

IV:1-2:7-8:II:3-4:9-10:III:V:5-6:I

The two plugs of Wheel A are in sockets IVa and Ivb.The first (or second) plug of Wheel B is in socket 1 and the second plug (or the first) is in socket 2, and so on ...

External-Key

The External key is the setting of the Wheel start positions. To avoid the setting of the ten wheels at each message, the key-table of the day (in addition of the inner-key) contains the start position of five wheel.

Example:

Wheel	A	B	C	D	E	F	G	H	J	K
March 4th	21	15	-	-	-	-	-	29	03	19
March 3rd	-	-	-	-	-	-	14	33	21	39
March 2nd	53	44	-	-	-	-	-	20	11	37
March 1st	66	20	42	04	-	-	-	-	-	28

The holes are filled by the cipher clerk with different values at each message. He send these positions before he set them in a sentence which starts by the string QEP.

Example:

"QEP 12 25 18 47 52"

If we are the 2 March, then the start positions of the wheel are: 53,44,12,25,18,47,52,20,11,37

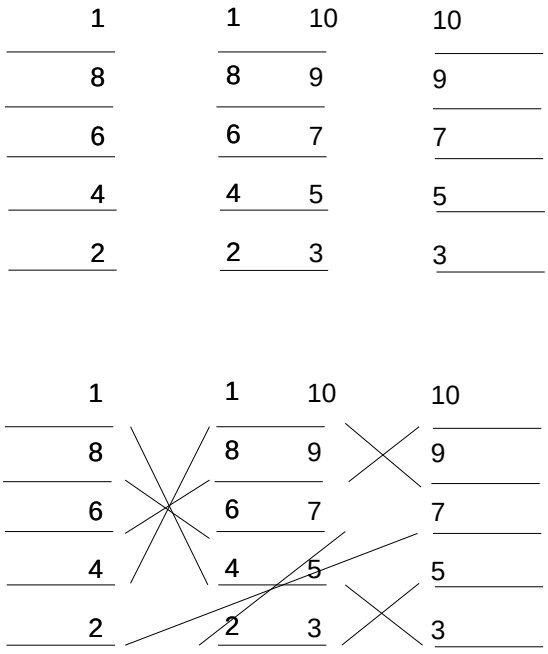
Chat

The cipher clerks exchange information between messages sent or received. This may be unimportant conversation ("how are you Siegred?") or the indication of the new message key, and finally the indication that they are moving from the clear mode to the encrypted mode or vice versa.

Example of changing message key: "QEP 12 25 18 47 52"
Example of swiching from plain mode to cipher mode: sender: "UNUM", ACK of receiver: "VEVE"
Other examples: "QRV ?" meaning "understood ?", sender: "ALLES KLAR ?", receiver response: "JA, HIER ALLES KLAR" (is everything clear ?, yes, everything is clear).

Because the cipher clerks only see plain text (even they work in cipher mode), sometimes, they exchange important information (for example message key) in plain mode.

The transposition cicuit



The transposition circuit (see picture) is configurable by plugs which connect permutation circuits. One of these permuation circuit permutes only two of the five lines (then two bits). If we connect the two plugs of one wheel in sockets 1 and 2, the lines (bits) 1 and 5 can be permuted (1-5).

Example: The plugs setting: 1-4, 6-8, 2-7, 9-10, 3-5 (see picture) correspond to the bits permutation (2-3), (3-5), (1-4), (1-2), (4-5).

Remark: not all configurations provide good configurations,
for example 1-10,8-9, 6-7,4-5,2-3 which provides the identical permutation [12345].

Cryptanalyse

Messages ciphered by the T52a/b are very difficult to break. Happily, often cipher clerks reset their machine before exchange a new message. After this, the Wheel start position are reset to their initial position (corresponding to the start of the last message). A lever of the machine permits this operation: the wheels come back to an initial position. As a result, many messages are superimposable (they are "in depth").