Description of Sturgeon (T52e model) cipher machine

Introduction

The T52e 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

The main-key switches, the SR and the Inner-key

Output from the wheels (Output Channel)

The ten bits keys (The Addition character and the Permutation character) come from ten wheels... but not directly!
The sensors of wheels read bits. One sensor read one bit (bit "a") and there is one sensor by wheel. We obtain the ten bits output from the wheels.

The main-key switches

Then the main-key switches mixes circuits. The input comes from the message key unit and then form the ten wheels (ABCDEFGHJK). These ten switchs (one switch by wheel) are labelled 1,3,5,7,9,I,II,III,IV,V. An electric circtuit forbides two wheels to occupe the same positions. For example wheels A and B cannot be associated to III position together. For each setting, the wheels operate on differents relays (SR1 to SR10).

Example of setting: 3, II, V, 1, 9, I, 7, III, 5, IV. The wheel A is in 3 position, the wheel B in II position, on so on, until the wheel K is in IV position. The wheel A (3 position) operates on SR1, SR4, SR7 and SR8. The relay SR4 is the sum (modulo 2) of bits from positions 1,3,5 and II.

The main-key switches

	1	3	5	7	9	I	II	III	IV	V
SR[1]:	X	X						X		X
SR[2]:						X	X	X	X	
SR[3]:			X	X				X		X
SR[4]:	X	X	X				X			
SR[5]:	X			X	X		X			
SR[6]:			X	X			X		X	
SR[7]:		X	X		X					X
SR[8]:	X	X				X			X	
SR[9]:					X	X		X		X
SR[10]:				X	X	X			X	

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 (or not steps) one sector. The wheels have a number of sectors first between them : (from K to A): 47, 53, 59, 61, 64, 65, 67, 69, 71, 73. 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
   12345678901234567890123456789012345678901234567890123456789012345678901234567
K="0101110010101110011101111000111010000111110001O"
J="0011100011100101110100001111000101101011011001101O110"
H="1111000110100011010110001111110011010110100111110001111O100"
G="1111010010011101011010110100001101001011101111000110011000101"
F="1011011110110011100001000011101111110001010101011111000010111100"
E="1111100101001101000010111110011101010110001010001000101111111O101"
D="0001001110011100101110001100100101111001000101101010001110000011O10"
C="0100001111011101110001001001110000110000110001011111010110010110000011"
B="0110111110000011100011011100000110101011100000101111001111110001000101O"
A="0111010101110011001110110000011100011110100000010110111000100110010011110"
   12345678901234567890123456789012345678901234567890123456789012345678901234567
```

Remark: For each Wheel, the sensor (bit "a" which controls ciphering) is before the benchmark which indicates 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 for one character ciphered (Position [bit "b"] and sensor [bit "a"] between parenthesis): [the bit "b" controls wheels stepping is read at "Position"]

K	J	H	G	F	E	D	C	B	A	10 Bits (a) and (b)	
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	(a)
										1 1 1 1 1 1 0 0 0 0	(b)

Inner-Key

The Inner key is the setting of ten switchs (one switch by wheel) labelled 1,3,5,7,9,I,II,III,IV,V. An electric circtuit forbides two wheels to occupy the same positions. For example wheels A and B cannot be associated to III position together.

Example of an Inner-key:
3, II, V, 1, 9, I, 7, III, 5, IV.

External-Key

The External key is the setting of the Wheel start positions. A key-list specifies sets of wheel start positions, each one is indexed by a double letter, for example FF is for 53 for the first wheel K.

Example:

QEP FF OO PP AA ZZ VV CC MM HH UU

Then the start positions of the wheel are: 53,44,12,25,18,47,52,20,11,37 for the wheels from K to A.

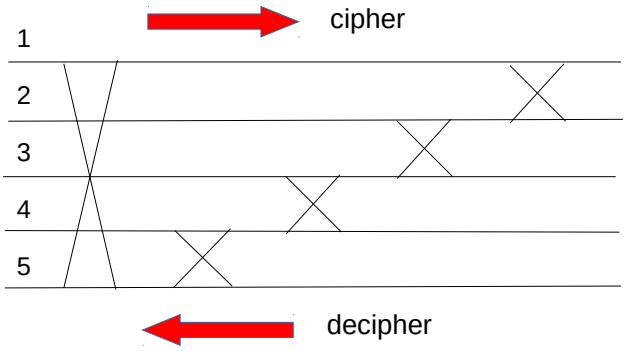
Chat

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 FF MM OO EE AA KK VV DD GG UU"
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 unit



The transposition unit can permute bit 1 and bit 5, bit 4 and bit 5, bit 3 and bit 4, bit 2 and bit 3, bit 1 and bit 2. We represent this by the formule (1-5), (4-5), (3-4), (2-3), (1-2)

Each transposition unit is materialized by a relay. The relay SR1 transposes bits (1-5), the relay SR2 transposes bits (4-5), the relay SR3 transposes bits (3-4), the relay SR4 transposes bits (2-3) and the relay SR5 transposes bits (1-2).

A key character actives or does not actives each of theses five permutations. The permutation takes place if the correspond bit is zero.

Examples

Key character	Permutation	Global
00000	(1-5), (4-5), (3-4), (2-3), (1-2)	15234
11111	nothing	12345
00101	(1-5), (4-5), - , (2-3), -	53214
10101	- , (4-5), - , (2-4), -	13254

Wheels stepping

The wheels step irregularly. The Wheels advance on the result of the modulo two addition of two other wheels, sometimes with inverted logic for one or both of the wheels.

Wheel A doesn't step if F and E (if bit "b" of wheel F is set to 1 and bit "b" of wheel E is set to 1).

Wheel B doesn't step if F and E.

Wheel C doesn't step if F and E.

Wheel D doesn't step if F and E.

Wheel E doesn't step if G and not F (bit "b" of wheel G is set to 1 and bit "b" of wheel F is set to 0).

Wheel F doesn't step if not G and not H.

Wheel G doesn't step if J and H.

Wheel H doesn't step if not J and K.

Wheel J doesn't step if A and not K.

Wheel K doesn't step if D and not E.