Report from Stanford University.
Added on the encryption scheme my personal notes.

One of the goals of the codebreakers at Bletchley Park was to break this Tunny machine to decrypt the messages of the German Army. Unfortunately this machine was much stronger than the known Enigma machine.

The Lorenz Shluesselzusatz consists of 12 wheels. The message to be encrypted or decrypted comes in as Baudot teleprinter code. Each bit is either a pulse or the absence of a pulse representing a cross or dot (1 or 0). Each character is decomposed into its five bits which are processed in parallel. Wheels are used to generate a pseudo-random keystream which is XORed with the plaintext bits. Each wheel has pins on it where each pin can represent two states, either a one or a zero. Thus a wheel is a bit sequence.

The Lorenz machine has two sets of wheels, a regularly stepping set called the Chi-Wheels and an irregularly stepping set called the Psi-Wheels. The wheels all have different periods which are relatively prime to obtain the largest possible number of wheel setting combinations. This ensures that the maximum length of a message is the product of the wheel lengths which is for the Chi-Wheels 23 x 26 x 29 x 31 x 41 = 22,041,682. This is long enough to ensure that a message is not encrypted more than once with the same keystream.

The irrugularly stepping Psi-Wheels are controlled by two motor wheels in series. The first motor wheel steps every time and the second motor wheel steps only if the first motor wheel is a one. The Psi-Wheels step only if the second moter wheel is a one.

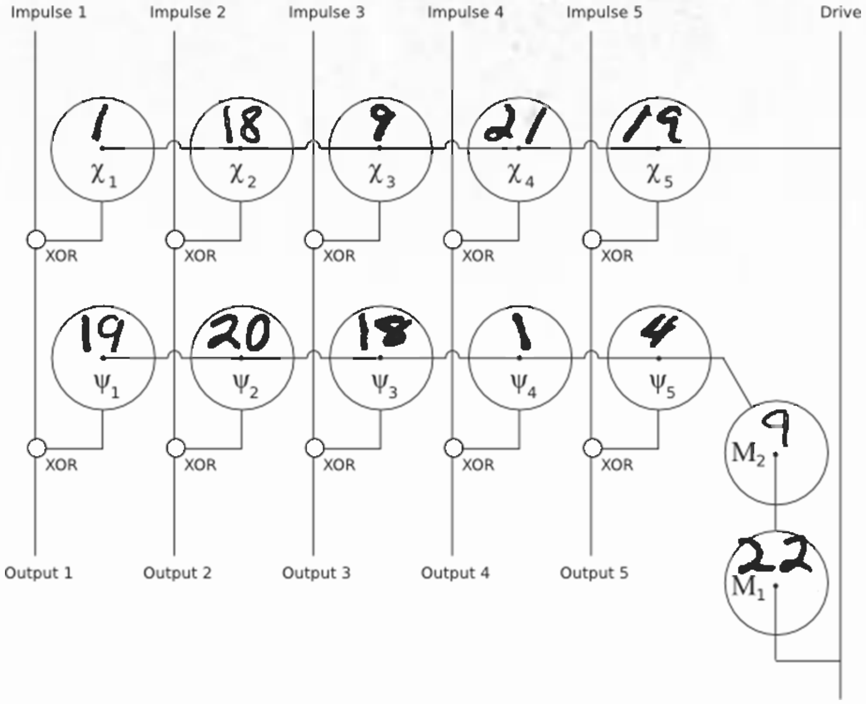
For the following analysis we denote the generated Psi-Wheel sequence with Psi'. This sequence is different from the wheel sequence since the wheels don't step every time.

The five Chi-Wheels and Psi-Wheels both produce 5-bit teleprinter letters which are XORed onto the incoming teleprinter message as shown in figure 1. Thus applying the theory of additive ciphers gives immediately as the keystream

$$K = \chi \oplus \psi'$$

and the encrypted message is

$$Z = K \oplus C.$$


Impulse 1
Impulse 2
Impulse 3
Impulse 4
Impulse 5
Drive
1
χ_1
18
χ_2
9
χ_3
21
χ_4
19
χ_5
XOR
XOR
XOR
XOR
XOR
19
ψ_1
20
ψ_2
18
ψ_3
1
ψ_4
4
ψ_5
9
M_2
XOR
XOR
XOR
XOR
XOR
22
M_1
Output 1
Output 2
Output 3
Output 4
Output 5