Baudot Code and Vernam

00011	A
11001	B
01110	C
....	
01000	CR
00010	LF

With Vernam cipher, and infinite, random key unbkreabkle.

How to get key?

(see http://www.codesandciphers.org.uk/lorenz/fish.htm)

Lorenz Machine

12 rotors:
- contain binary digits
- each has 23-61 positions

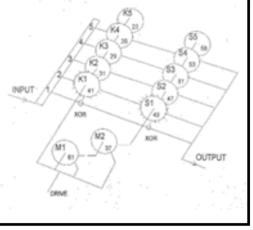
5 K-rotors
5 S-rotors
2 M-wheels

Key: initial setting of rotors

Encrypt 5 bits of plaintext with K-rotors
Encrypt the result with S-rotors
Advance all K-rotors by one position
Advance S-rotors according to M-wheels

Lorenz Machine (Fish)

- •First used by the Germans in 1940
- •The British did not have access to a Lorenz machine until the end of the war.
- •August 30th, 1941: two nearly identical messages (SPRUCHNUMMER vs SPRUCHNR) with 4000 characters encoded using same settings
- •John Tiltman and Bill Tutte managed to reconstruct structure of machine

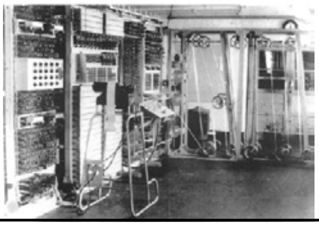


Tunny

Decryption was automated (Tunny machine), but settings had to be found manually, taking up to 6 weeks.

Newman/Flowers

- Mathematician Max Newman developed a computer to find settings automatically (based on Turing’s idea of a universal machine).
- Tommy Flowers built Colossus based on this idea, using valves rather than relays.



- First electronic computer (not stored-program)
- Consisted of 1500 valves
- Finished in 1943 at Post Office and shipped to BP
- 5000 characters per second