Bill Tutte
U of T to Waterloo.
History (culture).

War: 1939 fall
Bill Grad student in chemistry at Cambridge.
Not his forte. Already done math/ math
Saved from being a foot soldier.
As one applied to Bletchley Park. (BP)

BP: setup month prior to war.
Primarily to work on Enigma.

20-30? people worked
Hut in nbhd.

Bill interview 1941.
Went to "cipher school" at St. James Park in Jan. 1941. (3-4 mos,
learnt how to break codes of WWI.

Italian cipher "Hagelin Machine" (Not terribly difficult).
Used only for field operations. Only temporary Tutte could brea

Oct. 1941: Tapes from "Tunny" Machine Lorenz Machine
(FISH).

Teletype? (Typewriter: out comes tape from attachment)
Sent at high speed (over LAN lines then by wireless transmission).

Tutte.

FISH

Machines just being set up in 1941

Human error: Sent same message with same key.
slightly different however.
~4000 characters

Tutte only had the key added by FISH.

Wrote out key in different columns.

Some ideas about machine. Beginning had 12 letter code (maybe 12 wheels)
575 x 8 array from 4000 characters.
Interesting diagonals.

first wheel had 41 sprockets.
Two interesting wheels were associated w the first impulse. ?

Tutte developed statistical method to help decode FISH methods.
needed a computer before computers existed.

Still needed to know Key. approx #sprockets × 12 ~ 40^{12}.

Still focussed on first two impulses.
Vowels, 5's, t's would use less holes than Q or X or the teletype machine

"Heath-Robinson" machine at first. would break at high speed.
sneas "Ruth-Goldberg" machine

Max Newmann : Electrical Engineer. 1500 vaccum tubes
9 months.

Tommy Flowers: worked on switching systems for phone companies.

Enigma: Bombe. Electro mechanical device had some vaccum tubes.

Was built on "Dollis Hill"? (Not at Bletchley).
later moved to Bletchley & built at end of 1943 (moved to Bletchley Park).
∃ pictures.

Messages were long still useful even after a week / month.
↳ Coordination of groups of armies, bombers should be supplied etc.

Enigma very short messages.

* D-Day messages: British & Allied forces are going to land in Pas de Calais (Padeacalay).
Actually Normandy.
Used FISH decodes messages to know that enemy believed you would land in Pas de Calay

Collosus machine ?. This was the one shown above

Probably first machine over ENIAC.

Churchhill ordered machines to be destroyed after war.