CRYPTANALYSIS OF ENIGMA

GROUP NAME

ㄟ！那個嗎

GROUP MEMBER

資工一112550021林幼馨

資工一112550024陳芝瑄

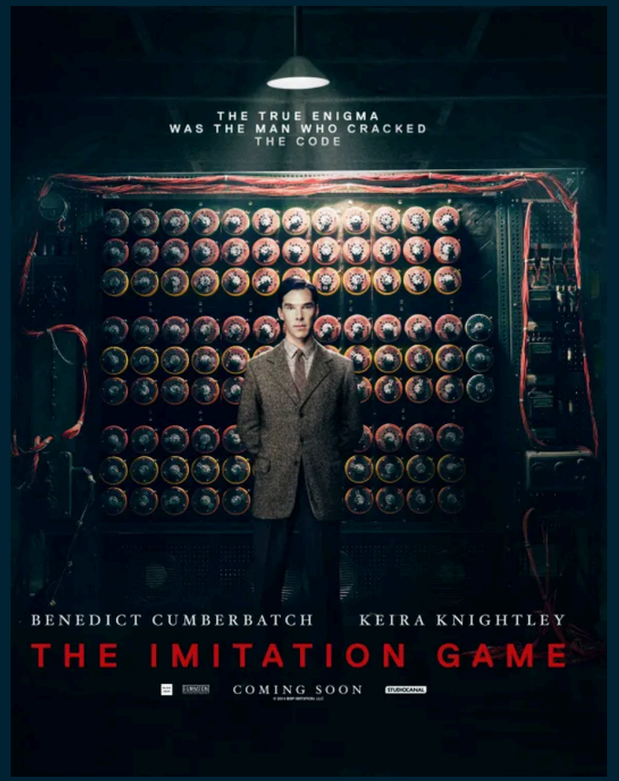
資工一112550090曾士珍

資工一112550173蘇宜盈

工工一112704039楊睿軒

INTRODUCTION OF ENIGMA

- Used by the German military during both World Wars
- Alan Turing designed the **Bombe machine** to decrypt it.



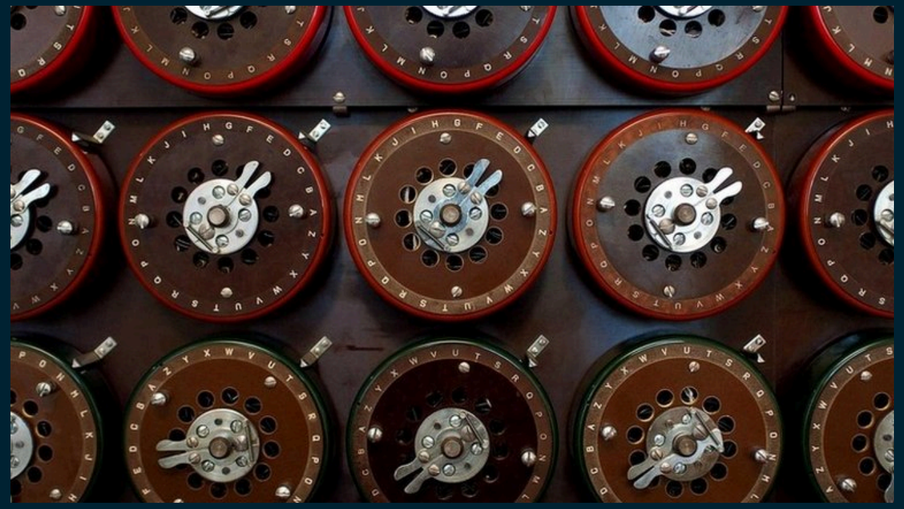
ENCRYPTION

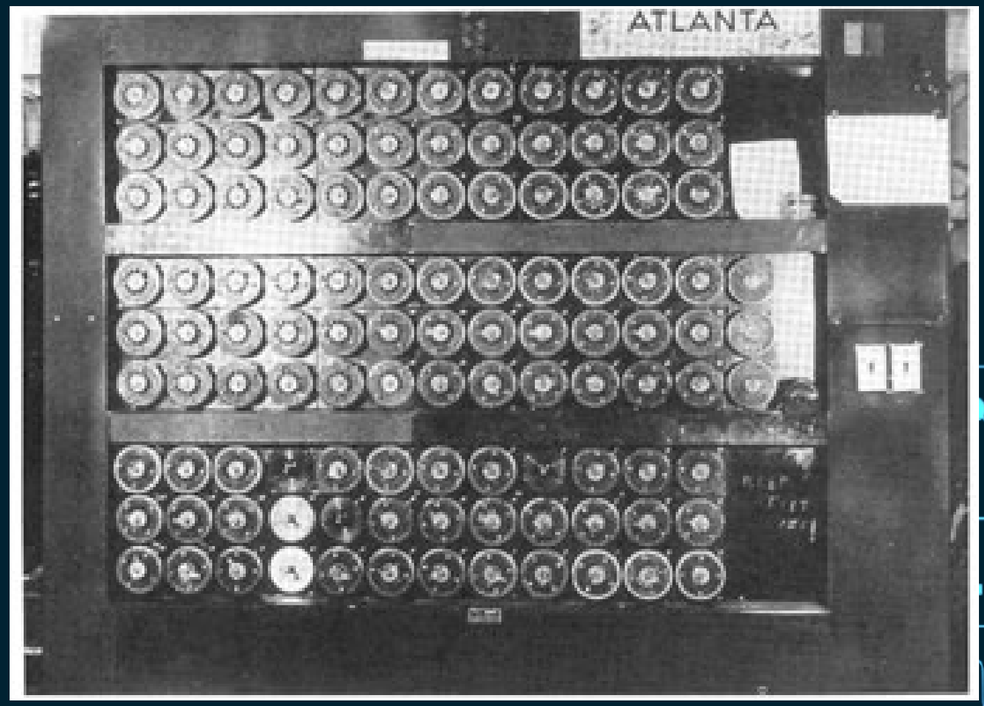
- Rotors : 5*4*3 = 60
- Starting set: 26^3 = 7576
- plugboard: 26!/(6! 10! 2^10)
- Paired two letters will be swapped

Total number : 158,962,555,217,826,360,000

Bombe machine

- Introducing a large quantity of electronic components
- Utilizing statistical principles, massively remove unnecessary search space





MARKOV CHAIN MONTE CARLO

Similarity Score Calculation

- find English-Similarity score of the text
- work on the log scale (for better numerical precision)
- probability table

Metropolis Algorithm

- new cipher produces text more similar to English than the current cipher -> accept
- otherwise -> accept / reject it with probability given by the ratio of their scores