

# Centenario Alan M. Turing

```
Dipartimento di Informatica  
Università di Milano  
enigmaduino @ sl-lab.it  
Twitter hashtag: #enigmaduino  
http://centenarioturing.di.unimi.it
```

## **Sessione divulgativa 9.00-10.30**

- Introduzione storica Alan M. Turing (Trentini, Pessina)
- Il contributo di Alan M. Turing alla Scienza dell'Informazione (Bertoni)
- La MdT come strumento per la divulgazione dell'informatica (Monga - Aladdin)

## **Sessione tecnica 10.30-12.00**

- Presentazione Enigmaduino (gruppo ArduinoAfternoon)
- Presentazione tentativi di cracking da parte dei solutori

# Alan Mathison Turing



23 giugno 1912 – 7 giugno 1954

Contributi per cui è noto:

- AI
- Enigma
- MdT

# Artificial Intelligence?

Can you read it?

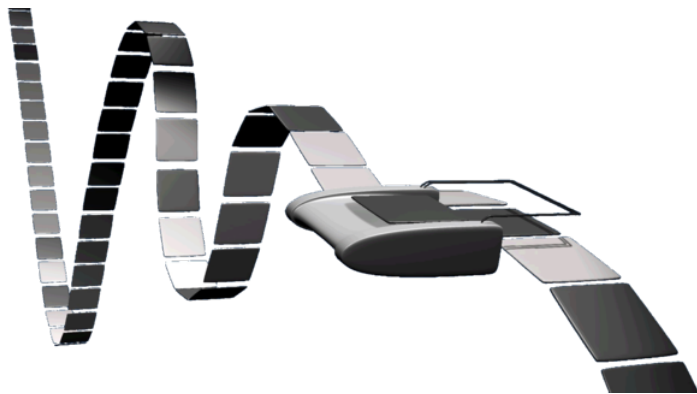


# CAPTCHA

```
**C**  ompletely  
**A**  utomated  
**P**  ublic  
**T**  uring-test to tell  
**C**  omputers and  
**H**  umans  
**A**  part
```

- Test di Turing, gioco dell'imitazione, Eliza
  - prima di lui Cartesio (Discorso sul metodo)
  - dopo di lui Philip K. Dick? (Voigt-Kampff)
- ... e Skynet: "Il sistema andò online il 4 agosto 1997. Skynet cominciò a imparare a ritmo esponenziale. Divenne autocosciente alle 2:14 del mattino, ora dell'Atlantico, del 29 agosto"

# MdT



(Bertoni, Monga)

# WWII

## Battle of the Atlantic



Donitz non era uno stupido...

# Wolfpack



Strategia di pattugliamento e attacco ai convogli navali

Pattugliamento "distribuito"

All'avvistamento seguiva una concentrazione

Però richiedeva MOLTA coordinazione... via radio!

Attacchi (all'attacco) possibili:

- radiogoniometria (fisico, analogico)
- codebreaking ("informatico")

# Enigma



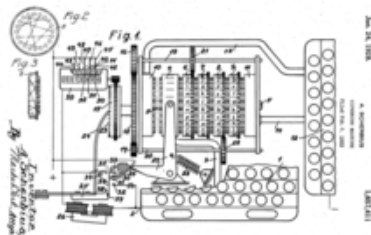
La credevano "unbreakable"... in effetti rispetto ai precedenti sistemi (Cesare, "bastoni", etc.) era molto avanzata - (VIDEO, da 45" in poi) funzionamento - ma...



# Bletchley Park

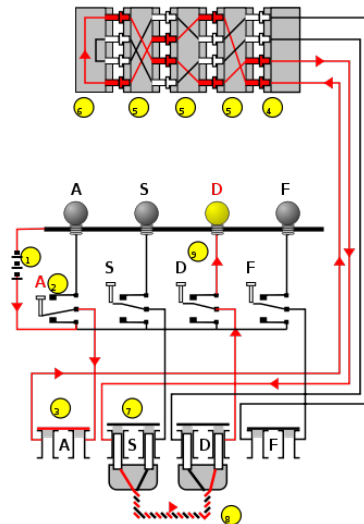
Affrontare il problema:

- conoscere il funzionamento
- conoscere o risalire al settaggio iniziale



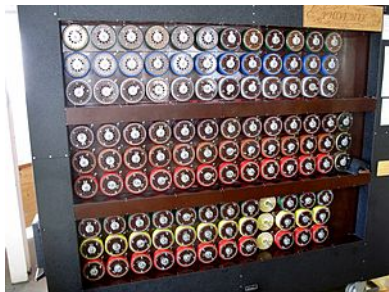
(libretti con i settaggi giornalieri)

# Dentro Enigma

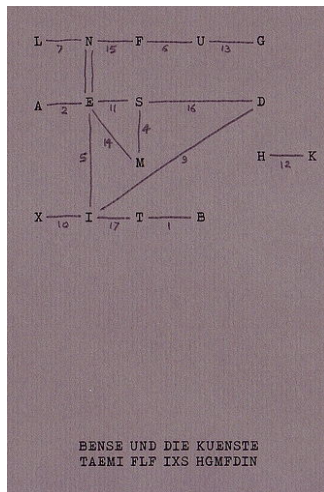


# Bletchley Park

- frequency analysis impossible
- needed clues (cribs)
- brute force



# Turing menu



## Altri eroi

Video documentario BBC (cfr. wiki centenario)

- William Tutte, matematico



- Tommy Flowers (Colossus)



"Disclosure" tarda (anni '80) e nemmeno ancora completata

Considerazione finale interessante, sociologica: approccio teutonico (ideologico?)  
vs. anglosassone (pragmatico?)

## Filmografia

- "From russia with love" 007 (spektor)
- U571 (ma la vera storia è quella dell'[U559](#): enigma machine AND codebooks)
- Enigma (molto romanzato ma interessante)

**The end**

**Q&A**

**GRAZIE!**