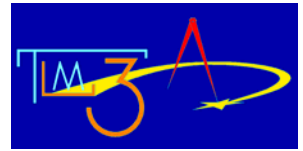




I.T.I.S. "E. DIVINI" San Severino Marche

PROGETTO COMENIUS TLM3
"Teaching and Learning Maths in the Third millennium"



ALAN TURING

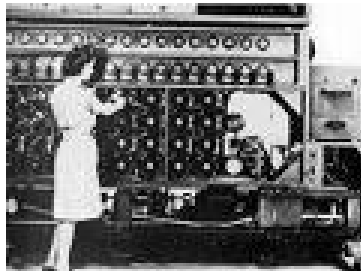
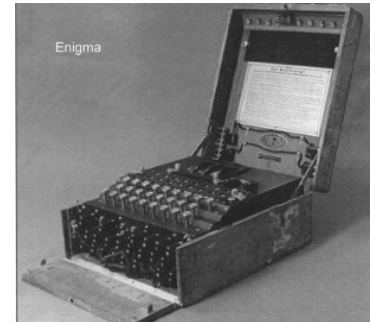
I SUOI STUDI - HIS STUDIES

LA CRITOGRAFIA (Enigma)

La più celebre macchina cifrante a rotori è l'Enigma inventata nel 1918 dal tedesco Arthur Scherbius e adottata dall'esercito e dalla marina tedesca anche nella seconda guerra mondiale.

La macchina ha al suo interno un certo numero di rotori (nella prima versione erano 3) collegati elettricamente e liberi di ruotare; la chiave dell'Enigma è la disposizione iniziale dei rotori, questa chiave veniva cambiata ogni 24 ore secondo una regola prefissata, in definitiva la vera chiave segreta era questa regola. Inoltre i tre (o più) rotori possono essere scambiati tra di loro, e quindi vi sono $n!$ ($3! = 6$ nella Enigma originale) disposizioni possibili, cosa che aumenta il numero di posizioni iniziali possibili. I tedeschi erano convinti che l'Enigma fosse inattaccabile, ma questa fiducia era assai mal riposta. Alan Turing ideò efficienti bombe crittologiche così che l'Enigma fu sistematicamente forzata. Nel 1942 si arrivò a decrittare più di 80000 messaggi cifrati tedeschi al mese!!

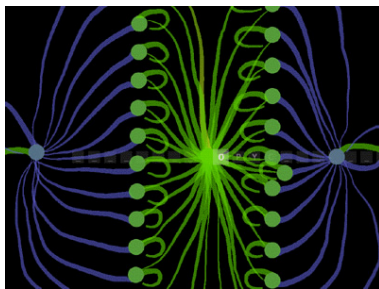
L'aver forzato, sin dall'inizio della guerra, l'Enigma (nonché altri cifrari tedeschi e giapponesi) fu un fattore di grande importanza per la vittoria prima della battaglia dell'Atlantico e poi degli anglo-americani nella II guerra mondiale.



THE CRYPTOGRAPHY (Enigma)

The most famous ciphering rotor machine is the Enigma, which was invented in 1918 by the German Arthur Scherbius. This machine was used by the German army and Navy in the second world war. Inside the machine there are some rotors (in the first version there were three rotors) electrically connected and free to rotate. The key of Enigma is the initial disposition of the rotors, this key was changed every 24 hours according to a fixed rule, after all the real secret key was this rule. Besides the three (or more) rotors may be exchanged among them selves, and so there are $N!(3!=6$ in the original enigma) possible dispositions, which increases the number of possible initial positions. The Germans were convinced that the Enigma was unassailable, but it was not. Alan Turing conceived efficient cracking bombs so that the enigma was systematically broken. In 1942 they managed to decipher more than 80000 coded German messages in a month! Breaking the Enigma (as well as other German and Japanese codes) since the beginning of the war, was of great importance for the first victory of the battle of the Atlantic and then for the Anglo-American victory in the second world war.

IL TEST DI TURING (e l'intelligenza artificiale)



Il Test di Turing è un criterio, introdotto da Alan Turing nell'articolo "Computing machinery and intelligence", apparso nel 1950 sulla rivista *Mind*, per determinare se una macchina sia in grado di pensare. Il test consiste in un gioco, noto come gioco dell'imitazione, a tre partecipanti: un uomo A, una donna B, e una terza persona C. Questo ultimo è tenuto separato dagli altri due e tramite una serie di domande deve stabilire qual è l'uomo e quale la donna. Dal canto loro anche A e B hanno dei compiti: A deve ingannare C e portarlo a fare un'identificazione errata, mentre B deve aiutarlo. Poiché C non possa disporre di alcun indizio (come l'analisi della calligrafia o della voce), le risposte alle domande di C devono essere dattiloscritte o similmente trasmesse.

Il test di Turing si basa sul presupposto che una macchina si sostituisca ad A. In tal caso, se C non si accorgesse di nulla, la macchina dovrebbe essere considerata intelligente, dal momento che - in questa situazione - sarebbe indistinguibile da un essere umano. Di qui nasce una disciplina che si occupa della "intelligenza artificiale", il suo scopo è la costruzione di una macchina in grado di riprodurre le funzioni cognitive umane. Sebbene le previsioni di Turing fossero che entro il 2000 sarebbe stata realizzata una macchina intelligente, finora nessuna ha superato il test.

TURING'S TEST

This test was introduced by Alan Turing in the article "Computing machinery and intelligence", published in "MIND" magazine in 1950.

It is a criterion used to determine if a machine is capable of thinking.

The test consists in a 3-player-game (also known as imitation game):

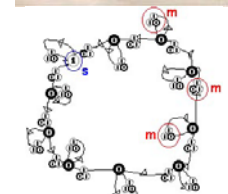
- a man A,
- a woman B,
- a third person C;

The third person C, separated from the others, must establish through questions which is the man/woman.

Also A and B have their tasks: A must deceive C in order to lead him/her to a wrong identification, while B must help him/her. In order to avoid leaving clues (such as voice or handwriting) all the answers to questions must be typed.

This test is based on the assumption that a machine replaces A. . . In that case if C doesn't find it out, the machine will be considered intelligent, as in this situation it is not distinguishable from a human being.

This is the origin of a new discipline which deals with artificial intelligence with the objective of building a machine capable of reproducing cognitive human functions. Turing estimated the building of an intelligent machine by 2000, but no machine has passed the test yet.



CLASSE 3 G