



IPPAZIA
V SEC.



AL-KHWĀRIZMĪ
IX SEC.



FIBONACCI
XIII SEC.



PACIOLI
XV SEC.



Galileo
XVI SEC.

GAUSS
XVIII SEC.



CANTOR
XIX SEC.



TURING
XX SEC.



EULER
XVIII SEC.



MÖBIUS
XIX SEC.



VON NEUMANN
XX SEC.

DI SILVIA SBARAGLI E ANDREA DE CARLI

TURING

MATEMATICI A FUMETTI

ZIO, NON NE AZZECCHI UNA! SIAMO FINITI IN MEZZO A UNA GARA DI CORSA!

NON MI SONO SBAGLIATO, MIA CARA! IL VINCITORE DELLA MARATONA È IL FAMOSO ALAN TURING!

OLTRE A ESSERE UNO DEI PIÙ GRANDI MATEMATICI DEL XX SECOLO, TURING È STATO ANCHE UN NOTEVOLE CORRIDORE E MARATONETA: HA OTTENUTO UN TEMPO DI SOLI 11 SECONDI SUPERIORE A QUELLO CON CUI IN QUEGLI ANNI SI VINCEVANO LE OLIMPIADI!

LA SUA FAMA, PERÒ, NON È DOVUTA ALLE DOTI SPORTIVE, MA ALLA GENIALITÀ IN CAMPO MATEMATICO, SOPRATTUTTO PER QUANTO RIGUARDA LA CAPACITÀ DI DECIFRARE MESSAGGI SEGRETI!

MA NON SONO MESSAGGI, SONO DELLE LETTERE E DEI NUMERI SCRITTI A CASO!

NO, CARA ELLIE. NASCOSTE IN QUESTE LETTERE E QUESTI NUMERI CI SONO IMPORTANTI INFORMAZIONI SEGRETE. GUARDA, STA DECIFRANDO I MESSAGGI DEI NAZISTI INTERCETTATI DALL'ESERCITO BRITANNICO!

HGR13

CCTHJ ELWIK

LWKR

IGQVD

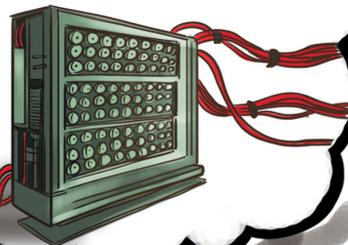
VJTNC

QX

LA MACCHINA ENIGMA DEI NAZISTI È UN VERO PORTENTO NEL CREARE MESSAGGI CRITTOGRAFATI ESTREMAMENTE COMPLESSI: SEMBRANO INDECIFRABILI.



PER VINCERE LA GUERRA BISOGNA DECIFRARE ENIGMA: CREERÒ UN'ALTRA MACCHINA PER BATTERLA!





TURING CI È RIUSCITO DAVVERO, ISPIRANDOSI A UNA MACCHINA IDEATA DA LUI CHIAMATA MACCHINA DI TURING.

VEDI, I NAZISTI SI INVIAVANO MESSAGGI TRAMITE ENIGMA...



E QUANDO GLI ALLEATI INTERCETTAVANO IL MESSAGGIO, TURING LO DECRITTAVA PER LORO GRAZIE ALLA SUA MACCHINA.



UNA STORIA DI SPIONAGGIO... MI PIACE!



ESATTO! IL SUO CONTRIBUTO È STATO FONDAMENTALE NELL'AUTARE GLI ALLEATI A VINCERE LA SECONDA GUERRA MONDIALE. È GRAZIE AI SUOI STUDI SUGLI ALGORITMI E SULLA SUA GENIALE MACCHINA CHE TURING È STATO POI CONSIDERATO IL PADRE DELL'INFORMATICA E DELL'INTELLIGENZA ARTIFICIALE.



TURING È STATO ANCHE IL PRIMO A PROGETTARE UN MODELLO TEORICO E CONCRETO DI COMPUTER, COME QUELLI CHE UTILIZZIAMO NOI OGGI. EBBENE SÌ, CARA NIPOTE! SENZA DI LUI NON AVRESTI I TUOI AMATI VIDEOGIOCHI!



NON POSSO TRADIRE LA MIA IPAZIA!

MA GRAZIE A TURING HO I VIDEOGAME! CHE DILEMMAAAA!



SÌ, TURING È STATO TRA I MATEMATICI CHE PIÙ HANNO CONTRIBUITO ALLA NOSTRA SOCIETÀ PRESENTE E FUTURA, E NON SOLO CON I VIDEOGAME! ELLIE, CHE FAI, ORA PREFERISCI TURING A IPAZIA?

DICIAMO CHE HO DECISO DI AVERE SPAZIO PER PIÙ DI UNA MATEMATICA O UN MATEMATICO PREFERITO...



DAI TEMPI DEGLI ANTICHI ROMANI A OGGI SONO STATI CREATI METODI DI CIFRATURA SEMPRE PIÙ COMPLESSI: IL FINE È RENDERE I MESSAGGI SEGRETI SEMPRE PIÙ DIFFICILI DA DECIFRARE DA PARTE DI NEMICI O AVVERSARI. UNO DEI PIÙ ANTICHI ALGORITMI CRITTOGRAFICI È IL "CIFRARIO DI CESARE": OGNI LETTERA VIENE SOSTITUITA CON LA LETTERA CHE SI TROVA UN CERTO NUMERO DI POSIZIONI DOPO NELL'ALFABETO. QUESTO CIFRARIO PRENDE IL NOME DA GIULIO CESARE, CHE LO UTILIZZAVA PER PROTEGGERE I SUOI MESSAGGI SEGRETI. ECCONE UN ESEMPIO, PROVATE A DECIFRARLO... **DYH FHVDUH** OGGI, INVECE, NELLA VITA DI TUTTI I GIORNI CI SCAMBIAMO MESSAGGI ATTRAVERSO SISTEMI ELETTRONICI (CELLULARI, COMPUTER ECC.) CHE COMUNICANO TRA DI LORO UTILIZZANDO SEQUENZE DI NUMERI. LA CIFRATURA UTILIZZA DELLE OPERAZIONI MATEMATICHE CHE SI BASANO IN PARTICOLARE SULLE PROPRIETÀ DEI NUMERI PRIMI. IL PRINCIPIO È QUELLO PER CUI DATI DUE NUMERI PRIMI ANCHE MOLTO GRANDI È POSSIBILE OTTENERE VELOCEMENTE IL LORO PRODOTTO, MENTRE NON È BANALE IL VICEVERSA, CIOÈ TROVARE I DUE NUMERI PRIMI CHE MOLTIPLICATI TRA LORO FORNISCONO UN DATO RISULTATO. IMMAGINATE CHE IL PRODOTTO DI DUE NUMERI PRIMI P E Q SIA 799 567, RIUSCITE A TROVARE P E Q? PER UN APPROFONDIMENTO SULLA VITA DI TURING, GUSTATEVI IL FILM DEL 2014 THE IMITATION GAME.

PER DECIFRARE IL MESSAGGIO "DYH FHVDUH" È NECESSARIO TORNARE INDIETRO DI TRE POSIZIONI: "AVE CESARE", I DUE NUMERI PRIMI IL CUI PRODOTTO È 799 567 SONO 839 E 953.