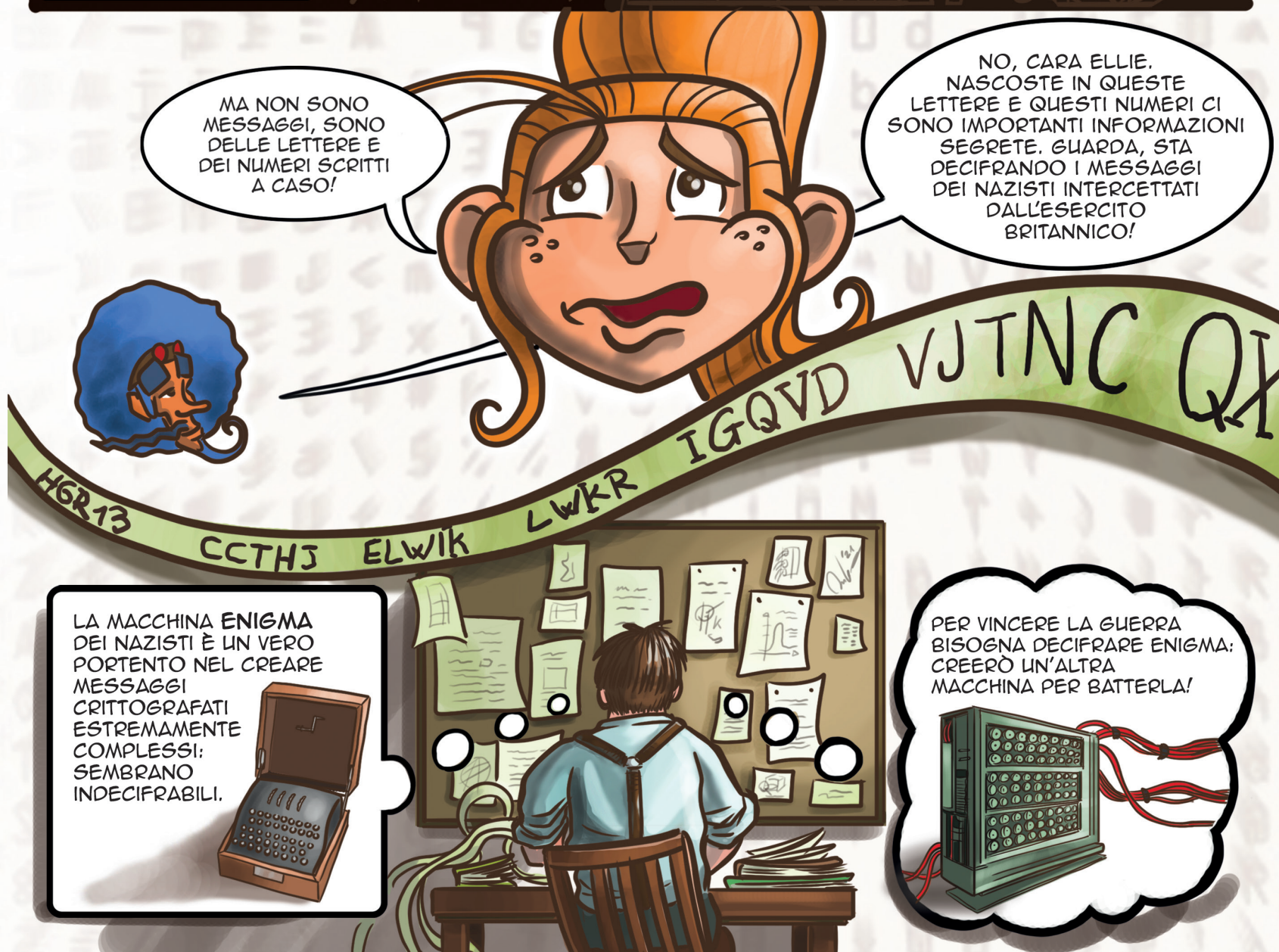
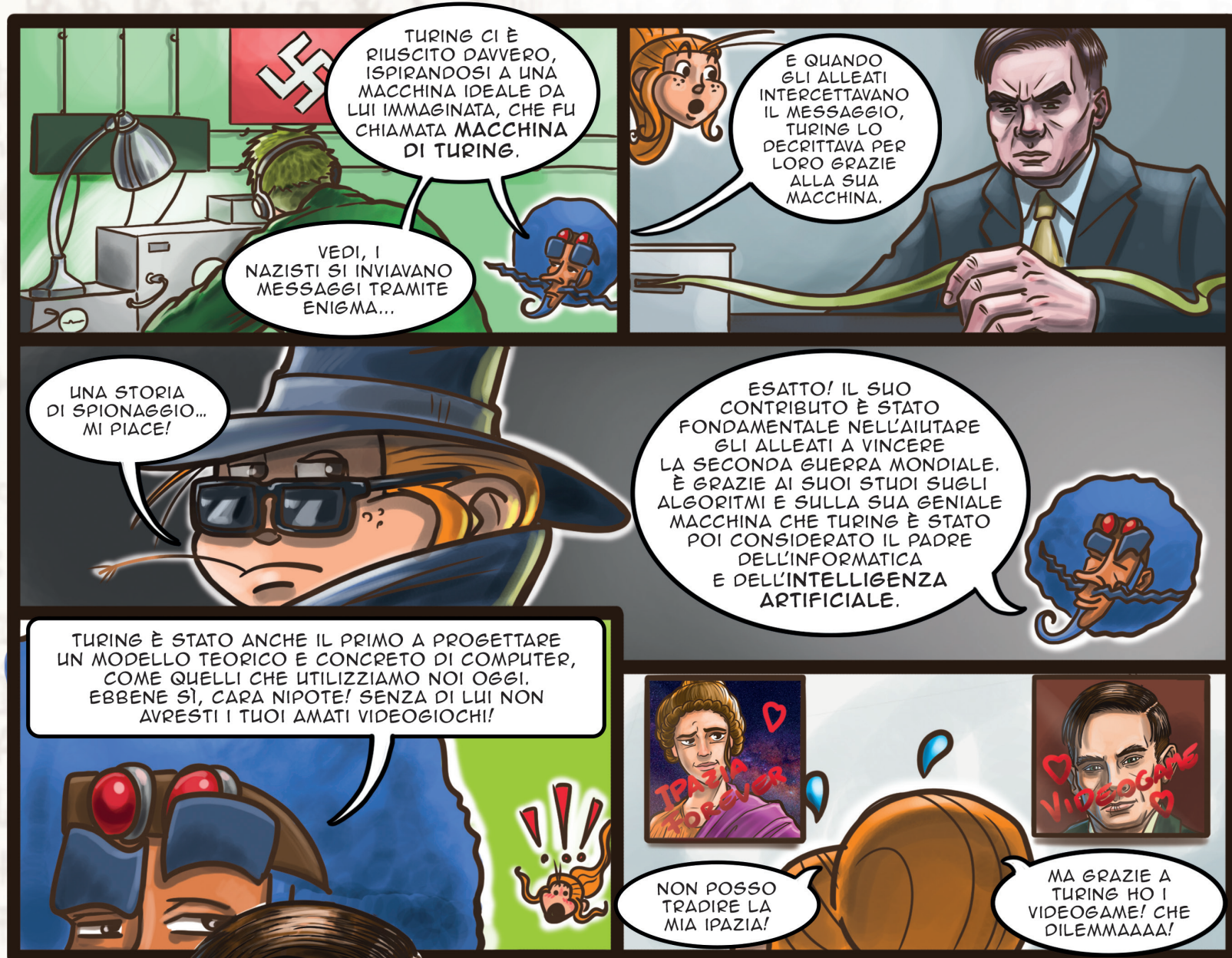


DI SILVIA SBARAGLI E ANDREA DE CARLI





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...

IPAZIA (E TURING!)

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.