12. Security e crittazione

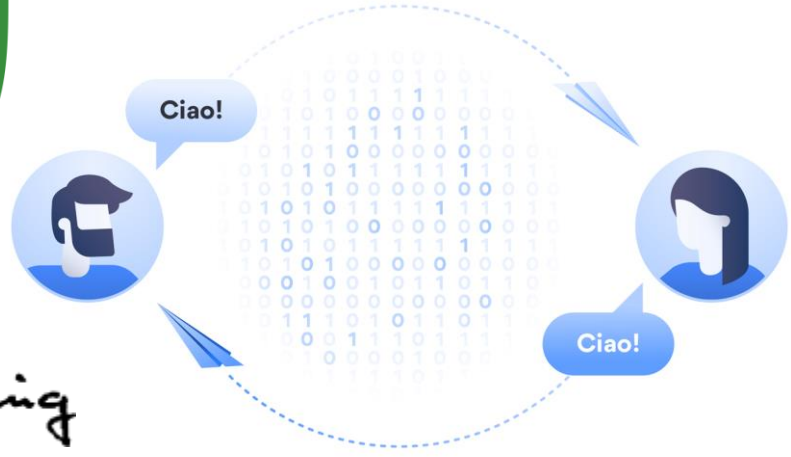
Università degli Studi di Trento

Sistemi informativi per il turismo

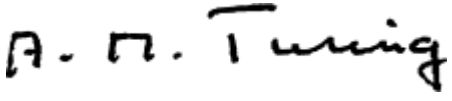
Anno accademico 2021-2022

Di che cosa parliamo oggi?

1. Privacy e security
2. Sicurezza della connessione
3. Sicurezza dei contenuti
4. Malware e hacking
5. Crittazione della connessione
6. Europa sicura
7. Alan Turing



immagini da דרכון פורטוגלי, Pixlr, Comodo Enterprise e NordVPN



Non è la privacy il primo problema, qui

Meglio dedicare un incontro specifico al problema della security, come la si chiama internazionalmente, e che in italiano, approssimando, possiamo chiamare sicurezza.

La security è spesso confusa con la privacy.

Effettivamente, in linea generale una connessione di rete sicura contribuisce alla "privatezza" – ammesso che questa parola esista in italiano – della trasmissione dei contenuti del messaggio.

Sono però due questioni differenti.

La privacy è un tema di diritti.

La security è una questione tecnica.

La condizione tecnica del caso è la crittazione.

immagini da Forbes India e ehorus.com

Messaggi in codice? Non soltanto.

Il concetto che sottende la crittazione è piuttosto semplice – rendere i dati illeggibili per chiunque, salvo che per utenti autorizzati identificabili.

In linea di principio si ottiene questo risultato usando la crittografia – lo studio di come spedire “messaggi” in qualche forma segreta, in modo che soltanto chi abbia autorizzazione a ricevere il “messaggio” sia in grado di leggerlo.

La parte semplice del processo classico di crittazione sta nell’applicare al testo in chiaro una funzione matematica che lo converta in testo cifrato.

La parte difficile sta nell’assicurare che chi abbia autorizzazione a ricevere il “messaggio” lo possa leggere facilmente, mentre soltanto chi sia autorizzato a ricevere il “messaggio” sia in grado di decifrarlo.

Ma la security riguarda anche la connessione, non soltanto messaggi cifrati.

File pericolosi

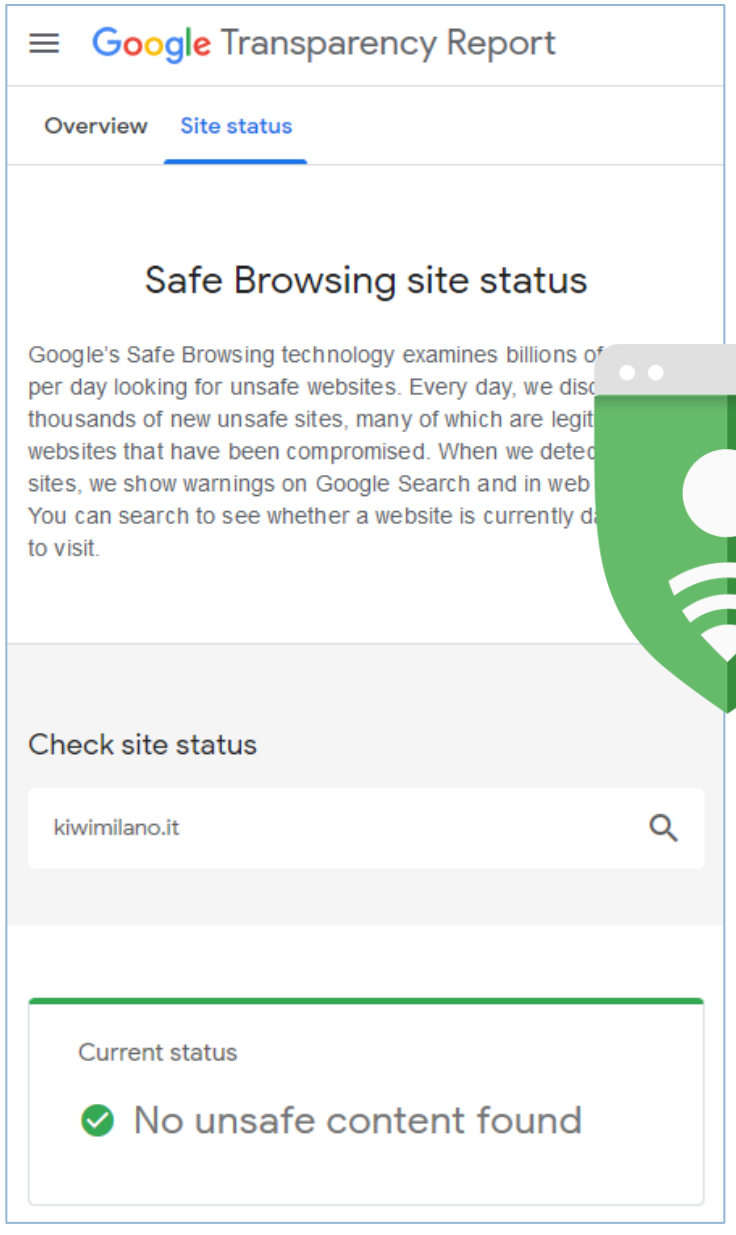
C’è però un’altra possibile confusione in agguato.

Può sembrare che, come per altre funzionalità, anche per questa il sistema Google offra un’opzione di verifica grazie a un online tool: uno strumento di rete.

Lo strumento on line che può sembrare garantisca la security è il Google Safe Browsing site status.

Non è così. Il Google Safe Browsing site status analizza la sicurezza dei contenuti di un sito.

La sicurezza dei contenuti è questione differente dalla security.



Malware

L'attacco a Yahoo! preparato e attuato nel 2000 da Mafiaboy – se ne è parlato a proposito di reti, perché la storia è riportata nell'introduzione a Linked – si basava sul fatto che Mafiaboy aveva infettato una quantità di computer con un malware programmato per far partire una richiesta (request) di negazione del servizio (denial of service) in un unico preciso istante. Questo aveva causato un istantaneo sovraccarico e un conseguente crollo (crash) del server Yahoo!

I computer si erano "infettati" perché avevano visitato siti web il cui contenuto non era sicuro – siti, cioè, contenenti file con istruzioni non richieste, celate e dannose.

Ma naturalmente non è che i gestori di quei siti avessero "infettato" loro i loro stessi siti!

Hacking

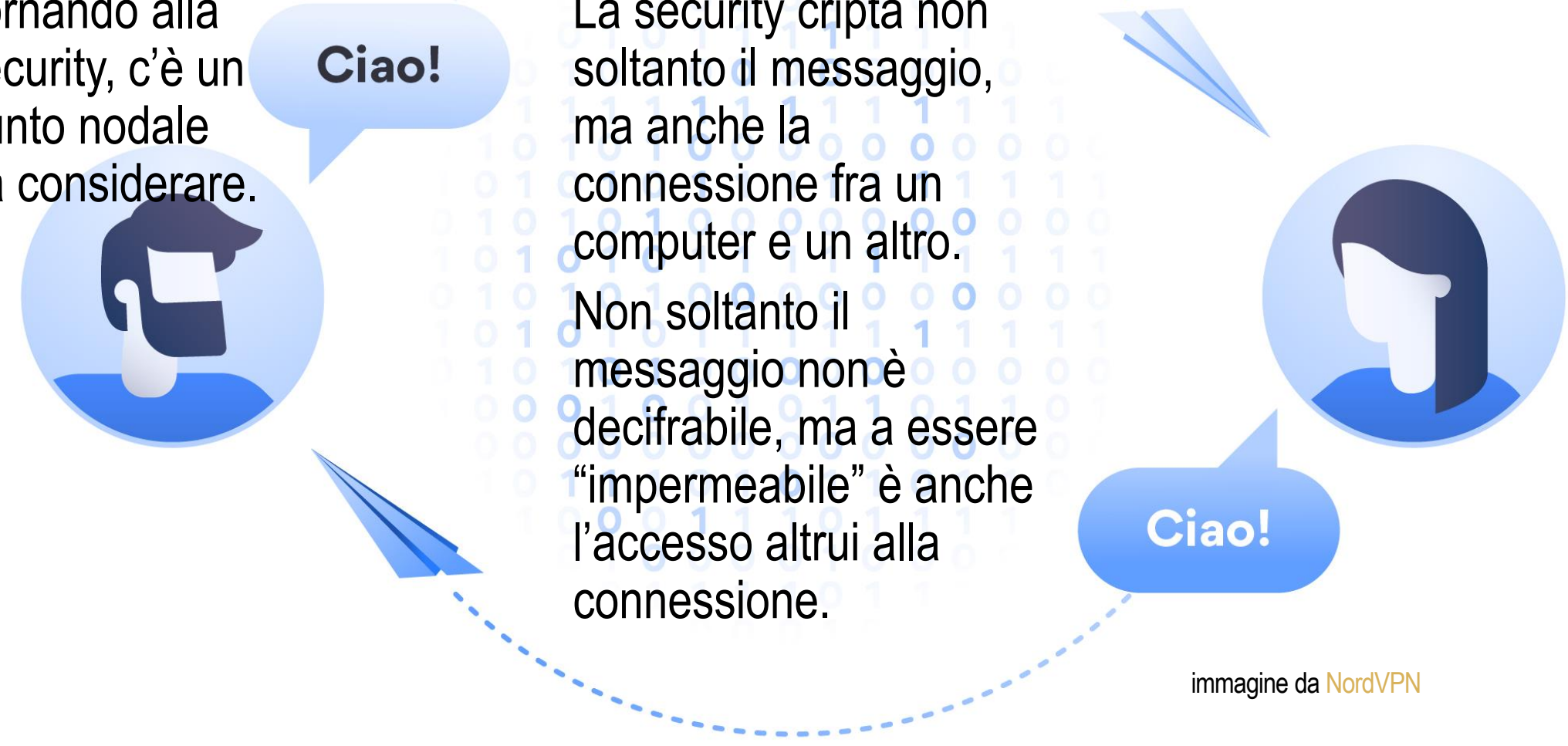
Mafiaboy era infatti un hacker – che poco più tardi avrebbe trovato lavoro come specialista nella sicurezza informatica – capace di fare in modo che i computer degli utenti, visitando un sito “infetto”, fossero surrettiziamente messi in contatto anche con un altro server diciamo così “infettante”. In casi del genere l’utente resta ignaro.

Ecco, ciò che fa il Google Safe Browsing site status è verificare che sul server di quel certo sito – che, appunto, si chiede di verificare – non siano presenti file con istruzioni non richieste, celate e dannose. Per farla breve, che non ci sia del malware.

È in sostanza una verifica analoga a quella che a ogni richiesta (request) fanno i software antivirus.

Crittazione della connessione

Tornando alla security, c'è un punto nodale da considerare.



La security cripta non soltanto il messaggio, ma anche la connessione fra un computer e un altro.

Non soltanto il messaggio non è decifrabile, ma a essere "impermeabile" è anche l'accesso altrui alla connessione.

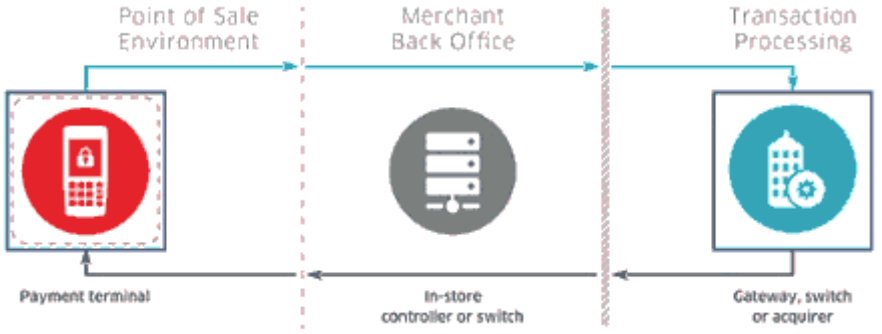
immagine da NordVPN

Lucchetti e https

Le connessioni criptate usano un protocollo di trasmissione specifico: non http ma https. Fra mittente e destinatario si interpone uno strato impenetrabile ad altri.

È la protezione che i browser evidenziano mostrando un lucchetto chiuso.

Crittazione finanziaria



I siti finanziari usano il protocollo https praticamente da sempre.

Il processo dell'e-commerce può iniziare in un sito a connessione magari non criptata (il sito un albergo, per esempio), dove l'acquisto si avvia. L'acquisto, però, si può perfezionare soltanto quando il processo si sposta in un sito finanziario (il sito di una carta di credito, per esempio) che sia protetto per pagare in condizioni di sicurezza.

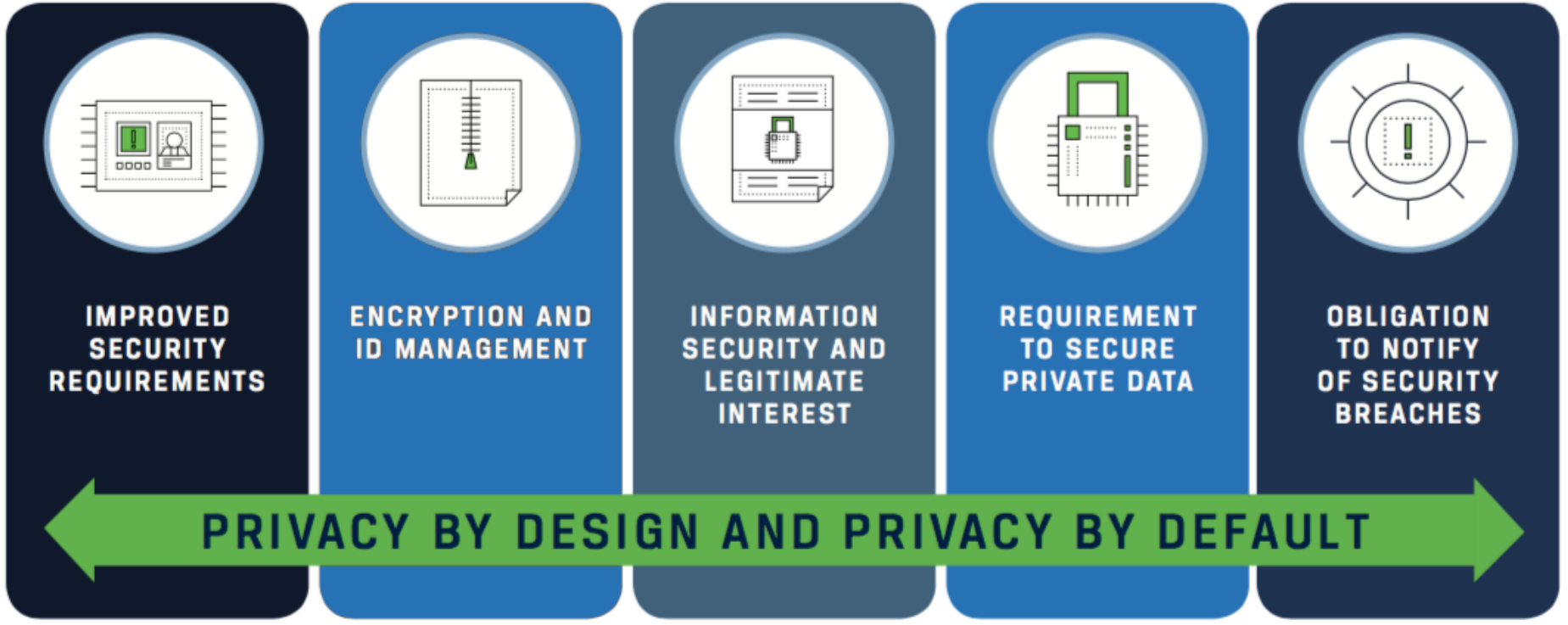
Una volta perfezionato il pagamento, il processo può rimandare al sito d'origine (magari non protetto) per certificare la transazione.

Che il processo fra il sito protetto e quello magari non protetto sia identificato (cioè che l'utente sia il medesimo) è garantito da cookie.

immagine da North American Bancard

Anche qui il GDPR

Le cose stanno così anche ora, ma la GDPR (EU General Data Protection Regulation) di fatto richiede che pure il sito d'origine (di un albergo, per esempio) sia criptato.



Google penalizza i siti non criptati, e usare l'https sta diventando l'approccio di default.

immagine da bankinfosecurity.com

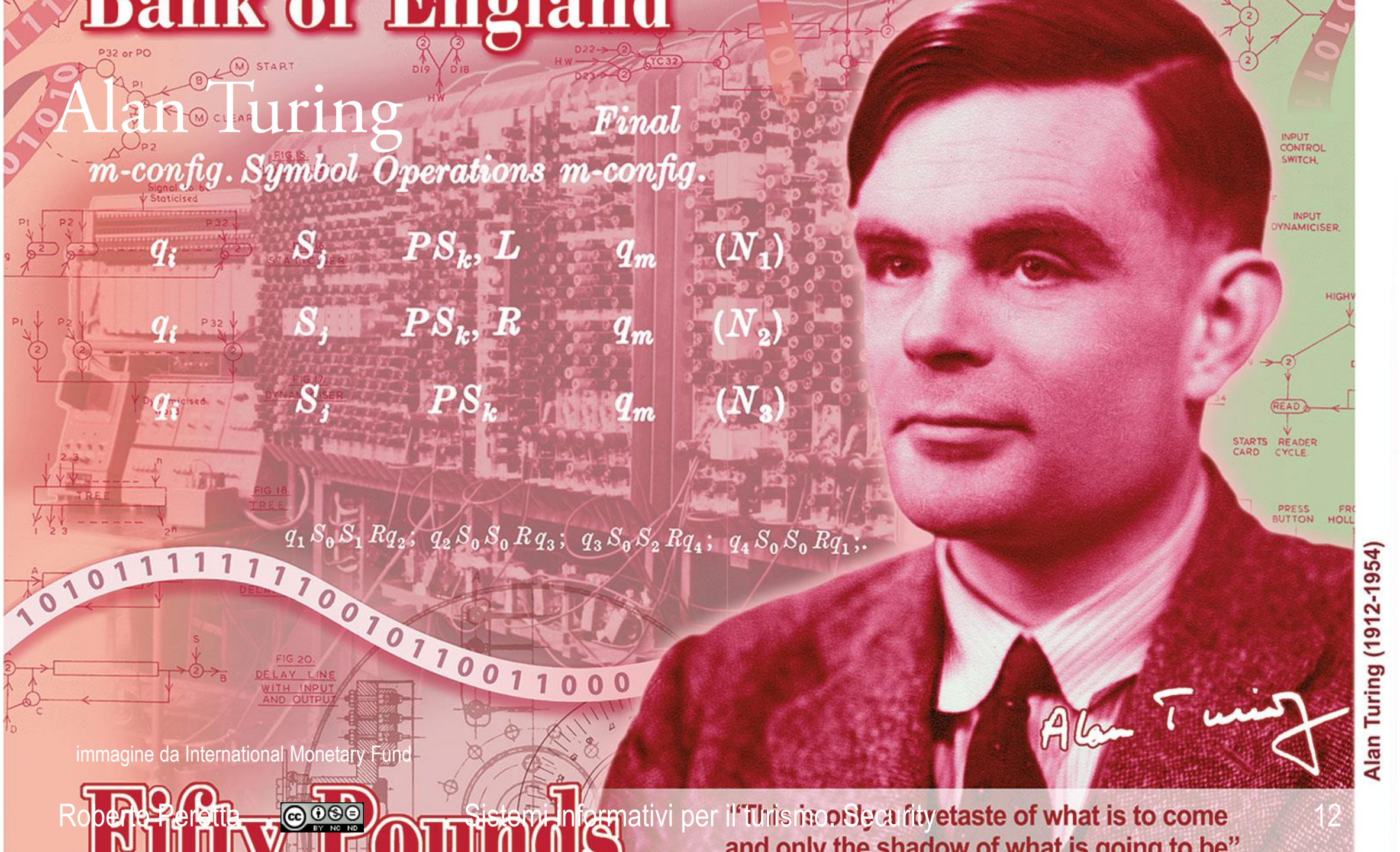


immagine da International Monetary Fund

Un padre dell'informatica

Introducendo il tema della crittazione, non si può non sottolineare che una vicenda legata alla crittazione sia stata fondamentale nella storia del calcolo computerizzato.

Si riprende qui di seguito un testo dall'edizione italiana di Wikipedia

"Il lavoro di Alan Turing (Londra, 1912-Manchester, 1954) ebbe vasta influenza sulla nascita della disciplina dell'informatica, grazie alla sua formalizzazione dei concetti di algoritmo e calcolo mediante l'omonima macchina, che a sua volta costituì un significativo passo avanti nell'evoluzione verso il moderno computer.

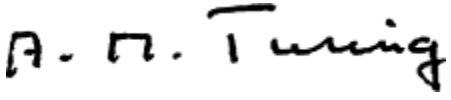
Per questo è considerato il padre della scienza informatica e dell'intelligenza artificiale, da lui teorizzate già negli anni trenta del '900, e anche uno dei più brillanti crittoanalisti che operarono nel Regno Unito durante la seconda guerra mondiale, per decifrare i messaggi scambiati da diplomatici e militari delle Potenze dell'Asse."

Bletchley Park

“Turing lavorò infatti a Bletchley Park, il principale centro di crittoanalisi del Regno Unito, dove ideò una serie di tecniche per violare i cifrari tedeschi, incluso l’utilizzo di una macchina elettromeccanica (chiamata ‘Bomba’) in grado di decodificare codici creati dalla macchina crittografica Enigma.

Turing morì suicida a soli 41 anni, in seguito alle persecuzioni subite da parte delle autorità britanniche a causa della sua omosessualità.”

È un’ironia della sorte – per usare un eufemismo – che un matematico così importante per la sconfitta di ideologie mortifere sia stato quasi letteralmente ucciso dalle leggi di una democrazia parlamentare.



I punti nodali di oggi

1. La security non è la privacy
2. ... e non è soltanto messaggi cifrati
3. Che cosa rivela Google
4. Protetta è anche la connessione
5. Che cosa rivela il lucchetto
6. Come non lasciarsi spiare
7. Un matematico martire

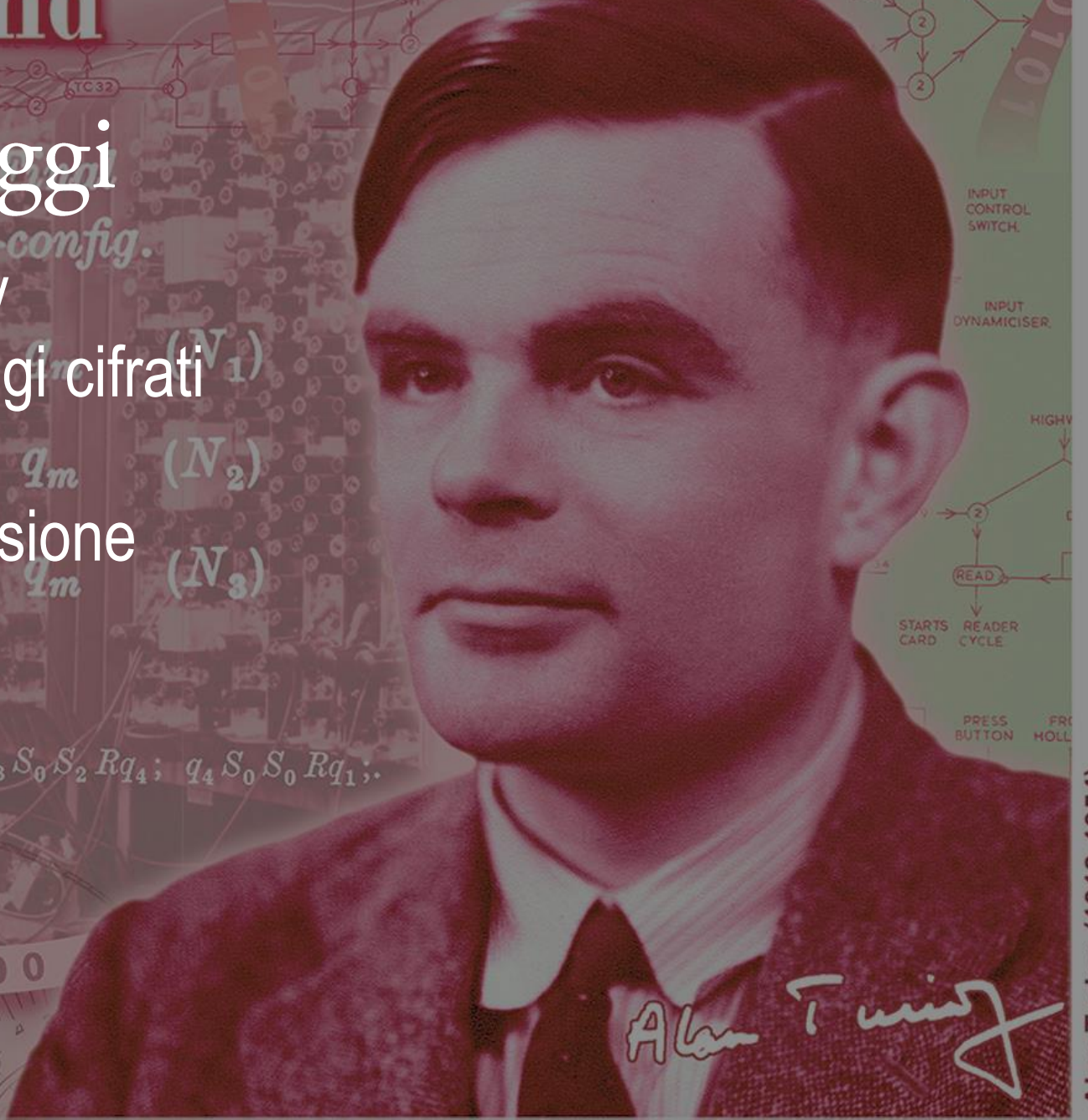


immagine da International Monetary Fund