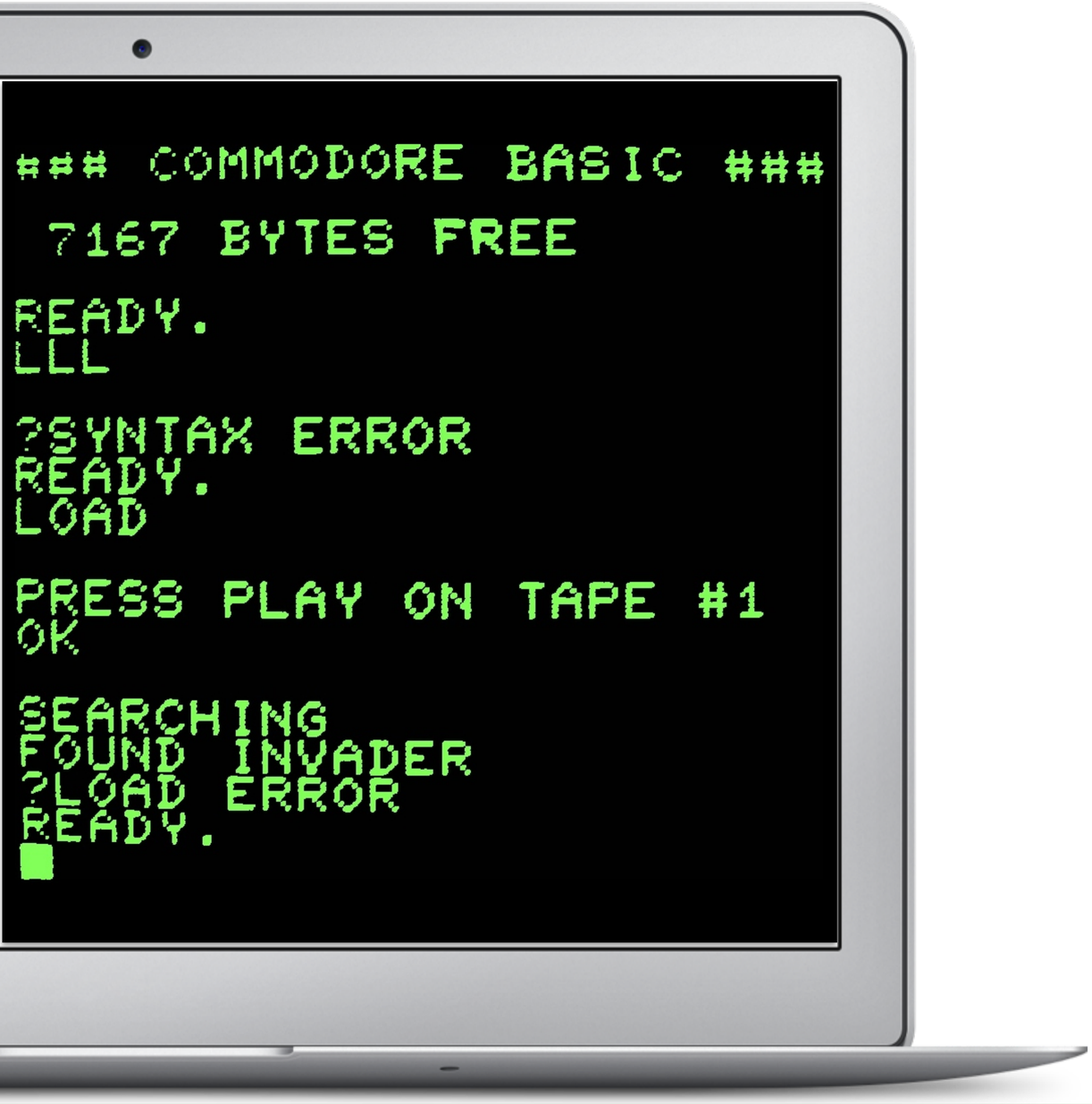


WELCOME

To The Net

Ovvero
sopravvivere ai dubbi da utente
ed altre storie

Crittografia

La crittografia è l'insieme delle tecniche atte a **rendere un messaggio incomprensibile** alle persone non autorizzate a leggerlo (un cosiddetto crittogramma).
La necessità di criptare un messaggio è molto antica, basti pensare che l'Atbash, il cifrario ebreo, viene citato anche nella Bibbia, nel libro di Geremia.

Grazie a questi sistemi, si garantisce la **protezione dei messaggi** scambiati tra mittente e uno o più destinatari, nei confronti di terzi non autorizzati (confidenzialità dei dati).

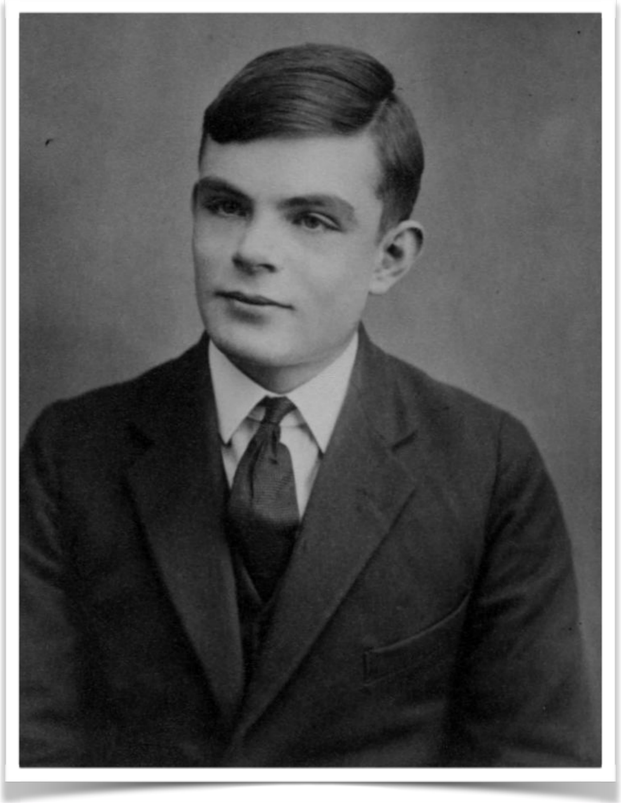
Crittografia

La tecnica inversa, ovvero quella usata per forzare una crittografia, si chiama **crittoanalisi**; essa non ha come scopo solo quello di decifrare un messaggio criptato ma anche di renderlo leggibile in tempi utili.

Decifrare un messaggio urgente in 50 anni non sarebbe utile, pertanto il tempo riveste un ruolo fondamentale.

Crittografia

Quella del tempo fu una delle sfide affrontate da **Alan Turing**, uno dei più grandi crittoanalisti che operarono durante la seconda guerra mondiale, per decifrare i messaggi militari dei membri dell'Asse; tali comunicazioni, identificando **obiettivi militari**,
dovevano essere rese leggibili prima degli attacchi nemici.



La storia di Turing è descritta nel libro
"Alan Turing: storia di un enigma"
di A. Hodges o nel film
"The imitation game"

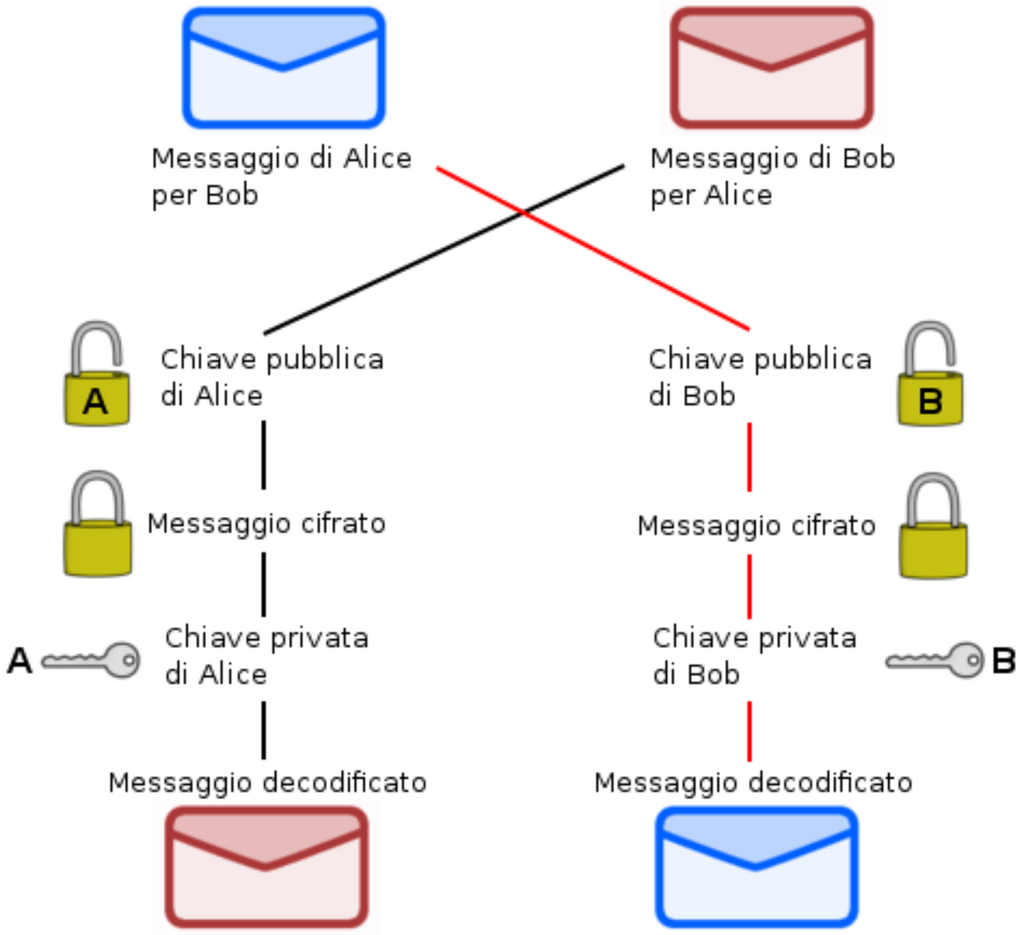
Crittografia

La **chiave crittografica** è il parametro utilizzato per cifrare e decifrare un informazione;
sulla base di ciò, vengono distinti due tipi principali di crittografia:

- Crittografia **simmetrica**
- Crittografia **asimmetrica**

La crittografia simmetrica usa **una chiave unica** per cifrare e decifrare il messaggio.
Il problema di questo sistema risiede nel riuscire a condivisione la chiave senza che essa venga scoperta da terzi.

Crittografia



La crittografia asimmetrica sfrutta **due chiavi diverse**; una chiave **pubblica**, con la quale è possibile cifrare un messaggio ed una chiave **privata**, necessaria per decifrarlo.

Crittografia

Nell ambito informatico, la crittografia trova **molte applicazioni**, basti pensare a mail, home banking, transito dati tra client e server, comunicazioni wireless o anche i programmi di messaggistica come Telegram o WhatsApp.

In una società dove attraverso internet vengono scambiati dati aziendali, comunicazioni di elevata importanza, transazioni monetarie ed informazioni riservate, poter contare su comunicazioni sicure che garantiscano la riservatezza, è **una priorità assoluta**.