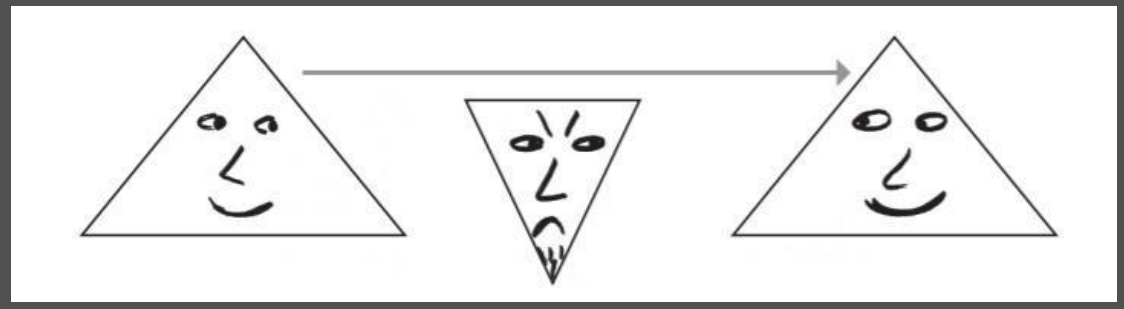
CRITTOGRAFIA

Che cos'è la crittografia?

- E' la scienza che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggi.
- **Crittografia** significa letteralmente «***scrittura segreta***».
- Con questo termine si intende oggi un insieme di tecniche che consentono di trasmettere messaggi mantenendoli segreti a tutti, tranne ad alcune persone che possiedano la chiave per comprenderli.



Proprietà della crittografia

- **Segretezza**

il messaggio non deve essere leggibile a terzi.

- **Autenticazione**

il destinatario deve poter essere sicuro del mittente.

- **Integrità**

il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.

- **Attendibilità**

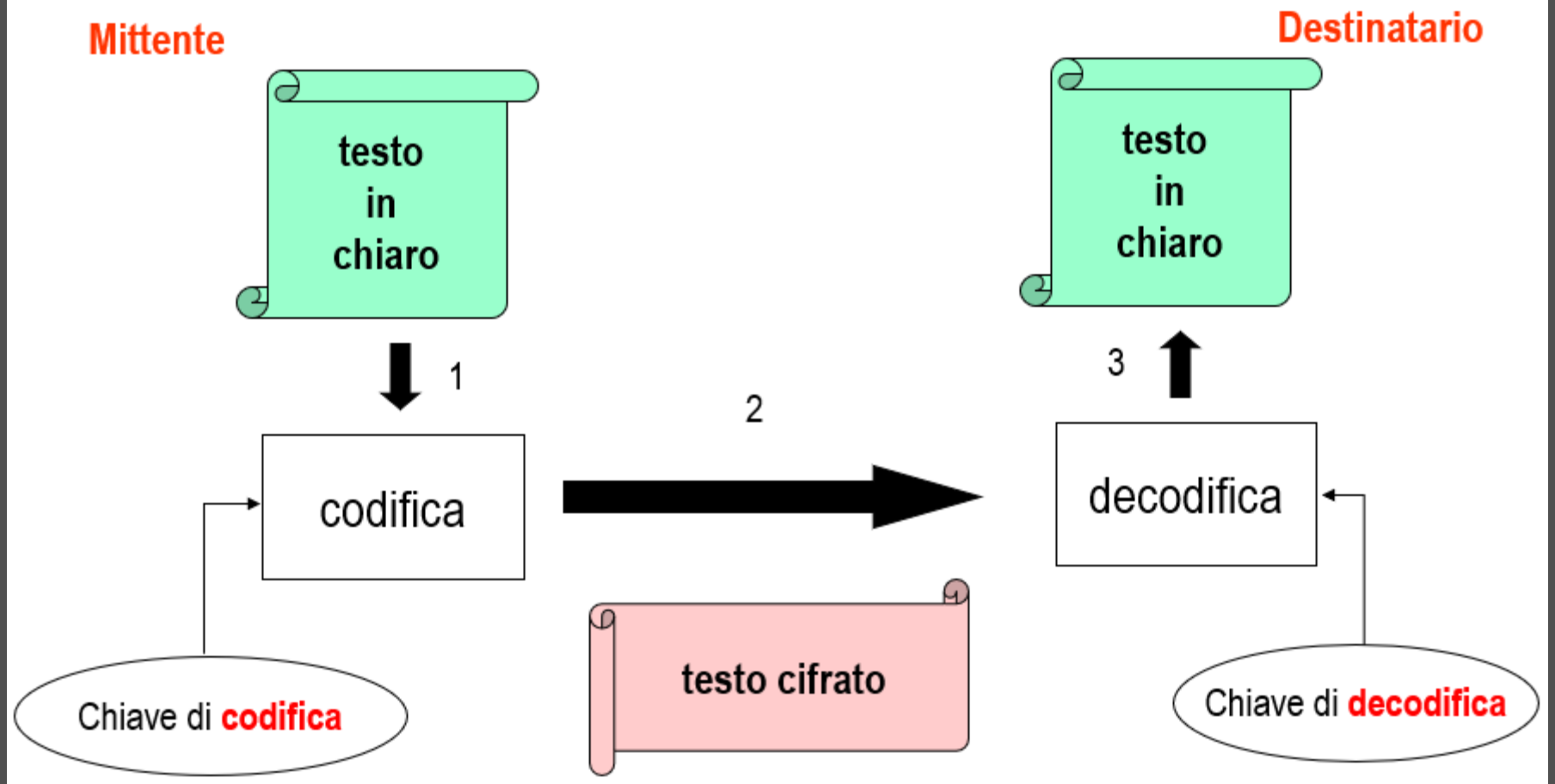
il mittente non deve poter negare di aver inviato il messaggio.

Un po' di definizioni….

- La **cifratura** è l'operazione con la quale si nascondono le informazioni; essa viene effettuata tramite un procedimento chiamato cifrario.
- **Il testo in chiaro** è il messaggio da cifrare.
- Il **testo cifrato** è il messaggio trasformato in modo da non essere più leggibile tramite una semplice lettura.
- La **decifratura** è la riconversione di un testo cifrato nella sua forma originaria, cioè nel testo in chiaro.
- Il **cifrario** è il procedimento (algoritmo) che consente di crittare e decrittare i testi.

- Il processo di cifratura deve essere biunivoco, in modo permettere un processo inverso che ritrovi il messaggio originale.
- Chi riceve il messaggio deve essere in grado di interpretarlo e cioè di decifrarlo.
- Il mittente ed il destinatario si devono essere messi d'accordo prima su come "cifrare" e "decifrare" e scegliere un metodo efficace in modo che per gli altri sia sostanzialmente impossibile cifrare e decifrare un messaggio.
- La crittografia fornisce metodi effettivi per effettuare cifratura e decifratura dei messaggi.
- Il processo di trasformazione dal messaggio in chiaro al messaggio cifrato e viceversa è spesso noto, ma si basa su una informazione specifica (detta "**chiave**"), senza la quale non si è in grado di operare.
- I metodi di cifratura si sono estremamente evoluti nell'arco della storia.

Codifica e decodifica



Utilizzo tradizionale della crittografia

- Gli usi tradizionali riguardavano quasi esclusivamente gli ambiti militari e di spionaggio/controspionaggio

- Sono riportati numerosissimi esempi di uso di sistemi crittografici nel corso di guerre, battaglie, rivoluzioni, cospirazioni, complotti, ...

Utilizzi moderni della crittografia

- L'uso più importante della crittografia in ambito "civile" è quella della sicurezza delle comunicazioni in rete

- Più in particolare le applicazioni di commercio elettronico sono quelle in cui maggiormente è sentita la necessità della sicurezza e della segretezza (scambio di dati sensibili, quali il numero di carta di credito, numero di conti bancari, ecc.)
- Un altro utilizzo importante è quello della firma digitale e dell'autenticazione dei documenti, che ha applicazioni nella pubblica amministrazione (e-government) e in generale negli aspetti burocratici (contratti, domande, moduli, vari documenti ufficiali, ecc.)

La crittografia nella storia
(dall'antichità al 1975)

Metodi antichi

- La scitala spartana
- La scacchiera di Polibio
- Il codice atbash
- Il codice di Cesare

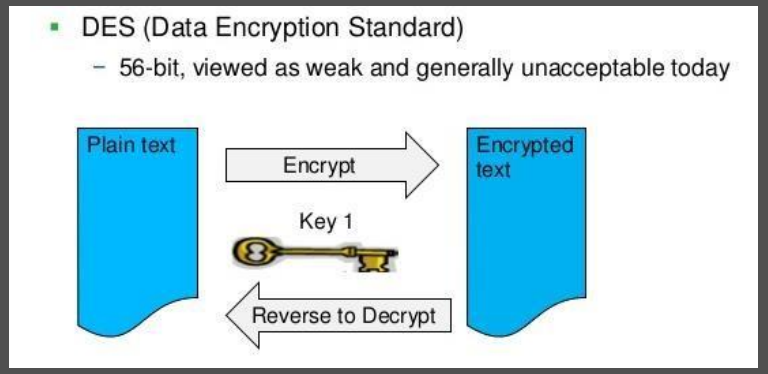
Rinascimento

- Blaise Vigenère

XX secolo

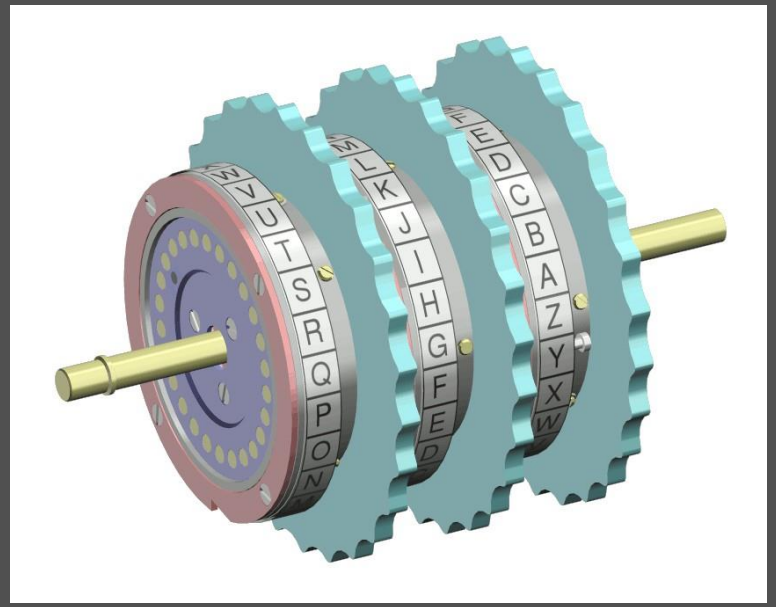
- La macchina Enigma (usata dai tedeschi durante la seconda guerra mondiale)
- Il DES (Data Encryption Standard)

Il disco cifrante di Leon Battista Alberti



Le macchine decifranti

Schema dei rotori della macchina Enigma



La storia di Enigma

Allo scoppio della seconda guerra mondiale nel 1939, gli alleati sapevano decriptare i messaggi di Enigma

Nell'agosto del 1939 gli inglesi installarono a Bletchley Park (80 Km da Londra) i servizi di Codice e di Cifrario.

Poco meno di 12000 scienziati e matematici inglesi, polacchi e francesi lavoravano per decifrare il codice di Enigma. Fra questi matematici, troviamo uno degli inventori dell'informatica moderna: **Alan Turing**, che dirigeva i lavori. I messaggi decriptati a Bletcheley Park arrivavano su dei nastro trasportatore alla *Huts 6*, poi, alla postazione per essere tradotti (due postazioni per squadra):

La storia di Enigma

Uno per i messaggi in ritardo;

Uno per il materiale urgente.

I messaggi tradotti della *Luftwaffe* erano trasmessi ai 3A e quelli dell'esercito ai 3M (A = aviazione; M = militare). Si attribuivano in seguito delle *Z* in funzione dell'importanza dei messaggi (*1Z*: importanza bassa; *5Z*: estremamente urgente).

La storia di Enigma

Gli inglesi riuscirono così a decifrare questi messaggi codificati.

Durante tutta la guerra, furono decriptati più di 18000 messaggi al giorno, e permisero alle forze alleate di conoscere le intenzioni della Germania.

L'ultimo messaggio cifrato fu trovato in Norvegia, firmato dall'**Ammiraglio Doenitz**: «il Führer è morto. Il combattimento continua».

I tedeschi non hanno mai dubitato che la loro preziosa macchina potesse essere decriptata.

Tipi di crittografia

SIMMETRICA

Si utilizza una sola chiave sia per cifrare che per decifrare i messaggi.

La chiave è conosciuta sia dal mittente che dal destinatario e deve essere mantenuta segreta.

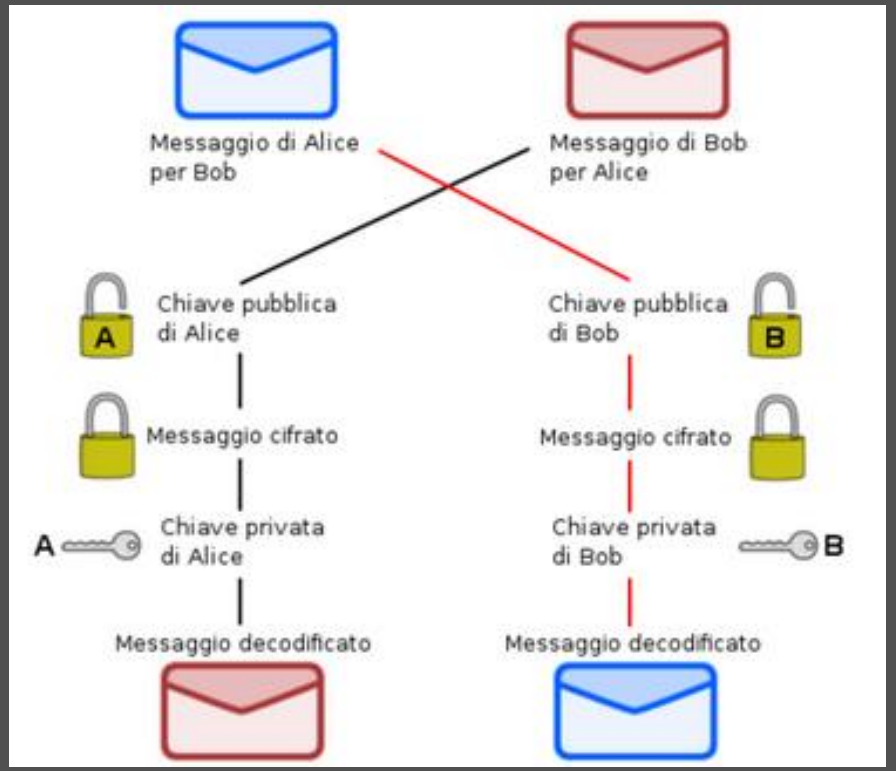
Tipi di crittografia

ASIMMETRICA

Si utilizza una coppia di chiavi, una per cifrare e l'altra per decifrare i messaggi.

Chiunque voglia trasmettere deve munirsi di entrambe le chiavi,utilizzando un programma per la loro creazione.

Una delle chiavi (**PUBBLICA**), è depositata nel registro di chiavi pubbliche in un server Internet.



ASIMMETRICA

Tipi di crittografia

La cifratura asimmetrica funziona a patto che la chiave pubblica sia certificata da un ente certificatore e che la coppia di chiavi abbiano la stessa lunghezza.

E' utilizzata per l'invio di un messaggio cifrato, per la non ripudiabilità del messaggio, per la firma digitale.

La cifratura asimmetrica è più lenta di quella simmetrica.