CRITTOGRAFIA

CHE COS'È LA CRITTOGRAFIA?

- La parola deriva dal greco **kryptós** "nascosto" e **graphía** "scrittura'';
- Abilità di scrivere messaggi in codice che non siano compresi da chi lo possa intercettare

SCHEMA INVIO MESSAGGIO:

Messaggio in chiaro → **CIFRATURA** → Messaggio cifrato o crittogramma → **DECIFRATURA** → Messaggio in chiaro

Estraneo che intercetta il messaggio e deve capire il modo per estrarre le informazioni.

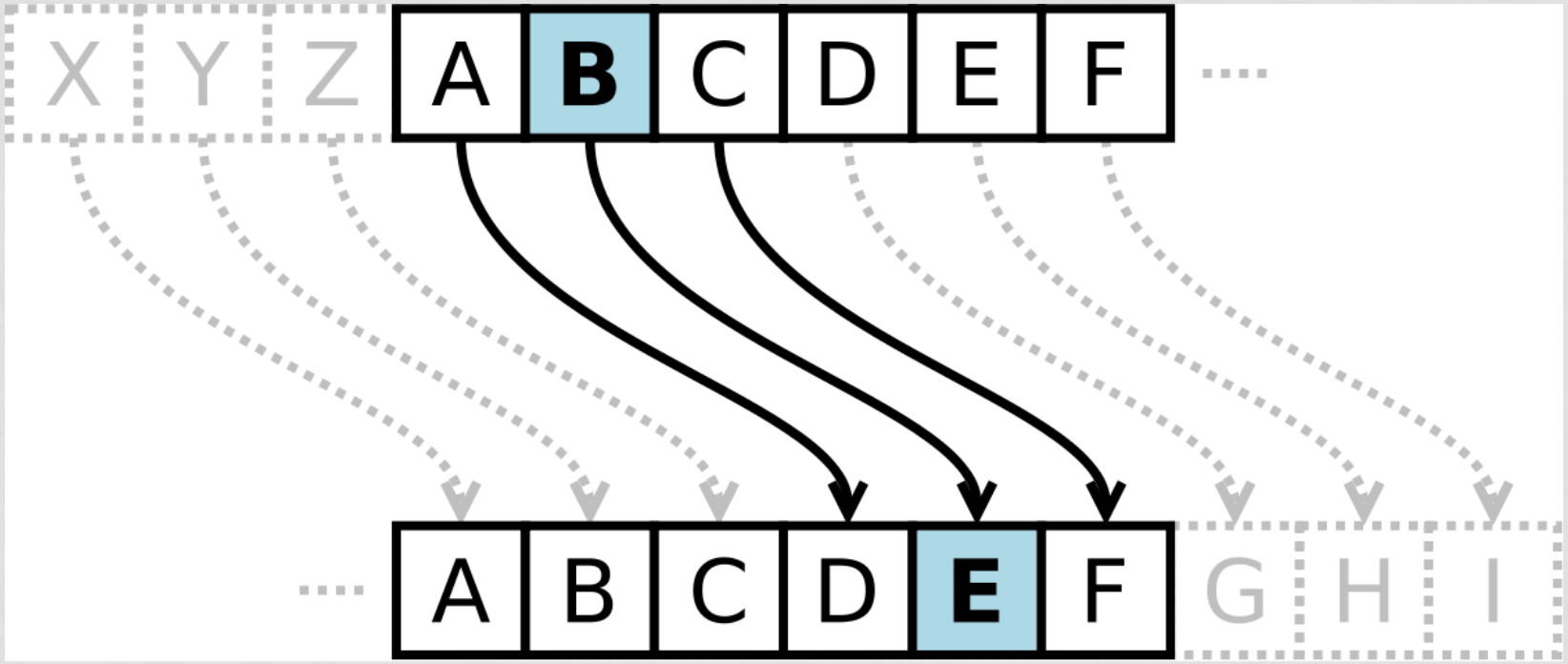
CRIPTAGGIO:

CRIPTAGGIO:

- Il mittente usa un **metodo** che deve rivelare al **destinatario** attraverso un codice detto **CHIAVE**;
- La **chiave** consente di associare ad ogni carattere del messaggio la lettera che esso rappresenta

CIFRARIO DI CESARE

- Lo storico **Svetonio** ci ha fatto conoscere uno dei più antichi algoritmi di cifratura il **''Cifrario di Cesare''**



CIFRARIO DI CESARE

- Alfabeto convenzionale utilizzato da **Giulio Cesare**;
- Sostituzione di ogni lettera con un'altra lettera esattamente quella che si trovata a **tre posti** di distanza nell'alfabeto normale;
- Detto cifrario a scorrimento;
- Utilizzato nella corrispondenza militare inviata alle truppe comandate da **Quinto Tullio Cicerone**.
- Al tempo era sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, figuriamoci uno cifrato;
- Non esistevano metodi di **crittoanalisi** in grado di rompere tale codice.

CIFRARIO LEON BATTISTA ALBERTI

- **Leon Battista Alberti** nel 1947 propose un metodo più evoluto;
- Utilizzava due dischi concentrici uno all'interno dell'altro uno fisso (esterno)ed uno mobile (interno);
- Disco esterno alfabeto normale con 20 lettere maiuscole e 4 numeri da 1 a 4;
- Quello interno con 24 lettere minuscole in ordine casuale caratteri utilizzati nel messaggio;
- Chi possedeva il disco sapendo di quante posizioni dovesse ruotare quello esterno poteva stabilire la corrispondenza;

CIFRARIO LEON BATTISTA ALBERTI

MACCHINA ENIGMA

- Seconda guerra mondiale i **Tedeschi** utilizzano ma **macchina enigma** per cifrare i messaggi.
- Basata su una serie di dischi (Leon Battista Alberti) messi in sequenza;
- Matematici polacchi, inglesi ma in particolare grazie ad **Alan Turing** con l'utilizzo dei primi elaboratori elettronici capirono i passaggi fondamentali per decriptare le informazioni.

MACCHINA ENIGMA

1. **TASTIERA**: immette la lettera in chiaro;
2. **UN'UNITÀ SCAMBIATRICE** che gira e cifra la lettera
3. **Un VISORE** con varie lampadine che indicano la lettera da inserire nel testo cifrato

CRITTOGRAFIA QUANTISTICA

- Messaggi che si trasmettono sotto forma di onde che se in **orizzontale** non passa dal dispositivo di ricezione quindi corrisponde allo **0** altrimenti passa in **verticale** e corrisponde all'**1**;
- Se il messaggio viene intercettato da una spia viene introdotto al messaggio una **perturbazione** (nota in meccanica quantistica);
- Le onde che prima erano solo verticali o orizzontali diventeranno **oblique** quindi il numero registrato non sarà recuperato con lo stesso numero di 0 ed 1 che attendeva il destinatario ma sarà diverso quindi saprà con certezza che il messaggio è stato intercettato.

CIFRARIO DI VIGENÈ

- Introdotto per la prima volta da **Giovanni Battista Bellaso** fu ritenuto per secoli inattaccabile, godendo di una fama in buona parte immeritata essendo molto più debole di altri cifrari polialfabetici precedenti.
- Invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave, da concordarsi tra **MITTENTE** e **DESTINATARIO**.

CIFRARIO DI VIGENÈ

Frase in chiaro:
ATTACCHIAMO

Chiave: **EMPOLI**

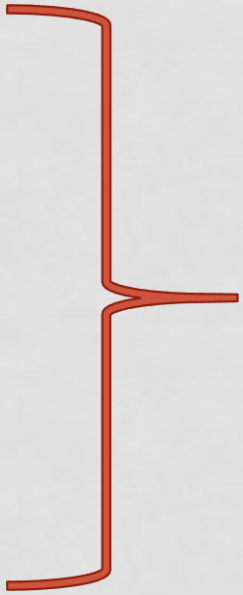
Messaggio combinato con chiave:
EMPOLIEMPOL

Messaggio crittografato:
EHMONMNVPCB

CIFRARIO DI VIGENÈ

Nella frase le lettere due **C**, due **T** e tre **A** del testo in chiaro vengono cifrate con lettere diverse:

- C→ N
- T → H
- T → M
- A → E
- A → O
- A → P
- C → M



Punto di forza dei cifrari polialfabetici e **punto di debolezza** dei cifrari monoalfabetici come il cifrario di Cesare

CIFRATURA SIMMETRICA

Intorno al 1800 **Kasiski** e prima di lui **Babbage** fornirono un metodo per individuare dapprima la lunghezza della chiave e successivamente il suo valore.

I metodi visti fino d ora fanno tutti uso di una **CIFRATURA SIMMENTRICA** ossia due persone utilizzano lo stesso codice, in gergo ''**CHIAVE''**, per cifrare e decifrare i messaggi che si scambiano.
In ambito informatico la crittografia simmetrica è molto debole nonostante si faccia uso di una chiave complessa perché il messaggio può comunque essere intercettato e rubato

CIFRATURA ASIMMETRICA

- Per ovviare al problema della cifratura simmetrica, nel 1976 **Diffie** e **Hellman** inventarono un metodo chiamato **CRITTOGRAFIA ASIMMETRICA**.
- Le due persone che comunicano non utilizzano solo una chiave, ma **due coppie di chiavi: una pubblica e una privata**. La coppia pubblica può non essere protetta, perché la sicurezza dipende dalla coppia di chiavi private.

COME FUNZIONA?

Il funzionamento è il seguente:

- **Davide** vuole inviare un messaggio a **Mattia**;
- **Davide** cifra il messaggio con la chiave pubblica di **Mattia**;
- **Mattia** riceve e decifra il messaggio con la sua chiave privata.
- I messaggi possono essere decifrati **solo** con la **chiave privata** corrispondente a quella pubblica che è stata utilizzata per la cifratura.

CRITTOGRAFIA END TO END WHATSAPP

La crittografia end to end fa un passo in più.

Per aumentare la sicurezza delle conversazioni, il sistema che gestisce il canale di comunicazione WhatsApp **non** controlla la creazione delle **chiavi private**, che vengono generate e archiviate direttamente sui dispositivi delle persone che comunicano.

Questo metodo di crittografia prende il nome di end to end, ossia "**dall'inizio alla fine**":

> **solo le persone interessate possono decifrare i messaggi e il flusso di comunicazione non coinvolge terze parti**.

Introdotta da WhatsApp nel 2016 per proteggere le conversazioni tra i propri utenti.

COME FUNZIONA?

- Quando aggiungiamo un contatto, le app di WhatsApp dei due dispositivi si connettono e creano **due coppie di chiavi interdipendenti**.
- Le **chiavi private** rimangono sui rispettivi dispositivi e sono **invisibili** anche a WhatsApp stessa.
- Quando invii un messaggio con WhatsApp, il server dell'azienda lo riceve e lo indirizza al destinatario, ma non è in grado di decifrarlo e leggerlo.
- Questo è il grande **punto di forza della crittografia end to end** applicata alle app di messaggistica istantanea e, in generale, alla comunicazione online.

QUALI SONO I VANTAGGI?

- Se un hacker attacca i **server del servizio di messaggistica**, ad esempio di WhatsApp, non potrà scoprire le chiavi private né accedere ai tuoi messaggi.
- **I tuoi messaggi sono visibili solo sul tuo terminale** e su quello del destinatario, per cui hai la sicurezza che **WhatsApp non registra le tue conversazioni e non le condivide** con altre organizzazioni (neanche con le forze dell'ordine).

QUALI SONO I LIMITI?

- La crittografia end to end è molto sicura, ma non infallibile.
- **Non esistono sistemi di sicurezza infallibili**.
- Se un hacker non può decifrare un messaggio codificato con la crittografia end to end, può accedere alle conversazioni in altri modi indiretti.
- Può utilizzare tecniche per accedere all'account di archiviazione online in cui l'utente salva il backup delle conversazioni. Oppure può infettare il dispositivo con
- un **keylogger**, un virus che registra gli input inseriti con la tastiera.