Modulo 13

Laboratorio

Ricercare in rete La storia del matematico inglese Alan Turing.

Far riflettere su come Il matematico Turing, con le sue competenze matematiche, ha contribuito alla vittoria degli eserciti alleati durante la seconda guerra mondiale.

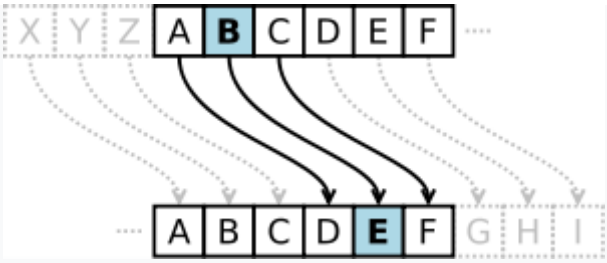
Tempo 30 minuti

Lezione frontale

Il problema di passare informazioni riservate è stato sempre presente nella storia dell'uomo. Nell'antica Grecia si usava la scitala

La **scitala** o **scitale** (in greco antico: σκυτάλη, *skytàlē*, "bastone") è considerato tradizionalmente un messaggio cifrato e segreto che veniva inviato dagli efori, i cinque supremi magistrati di Sparta, ai generali e ai navarchi impegnati nelle spedizioni militari.[1] Si tratta di uno dei più antichi metodi di crittografia per trasposizione conosciuti: il meccanismo di codifica permetteva, nel caso la scitala fosse stata intercettata dal nemico, di mantenere segreto il contenuto del messaggio e, nello stesso tempo, consentiva al ricevente di verificarne l'autenticità, in quanto solo chi era dotato di una bacchetta identica a quella utilizzata dal mittente per preparare la scitala, poteva decifrare e leggere il messaggio.[2]

Anche nell'antica Roma era necessario un metodo sicuro per impartire ordini agli eserciti, Cesare ideo' il suo cifrario. In crittografia il **cifrario di Cesare** è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. Questi tipi di cifrari sono detti anche **cifrari a sostituzione** o **cifrari a scorrimento** a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.



Il cifrario di Cesare è stato usato fino al 1400. Dopo è stato sostituito dal cifrario di L.B. Alberti che fondamentalmente funziona con lo stesso metodo, ma complica la sostituzione delle lettere.

Un disco cifrante di Leon Battista Alberti[1]

In crittografia il **disco cifrante** di Leon Battista Alberti, descritto nel *De cifris* intorno al 1467, è il primo sistema di cifratura polialfabetica. L'apparecchio si compone di due dischi concentrici, rotanti uno rispetto all'altro, contenenti un alfabeto ordinato per il testo in chiaro (testo da cifrare) e un alfabeto disordinato [2] per il testo cifrato (testo risultante). Permette la sostituzione polialfabetica con periodo irregolare. Lo scorrimento degli alfabeti avviene per mezzo di lettere chiave inserite nel corpo del crittogramma.

Tempo 90 minuti