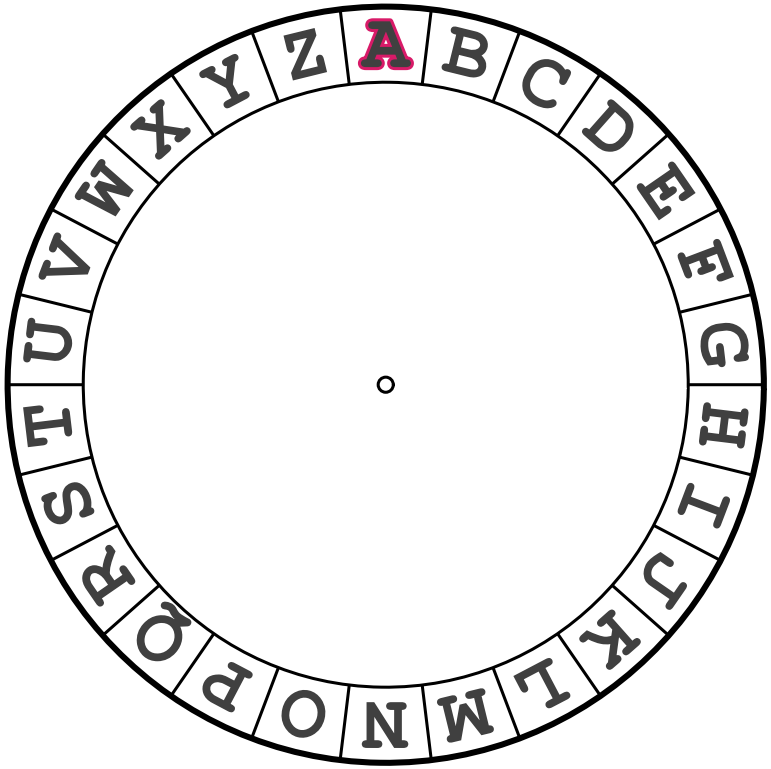

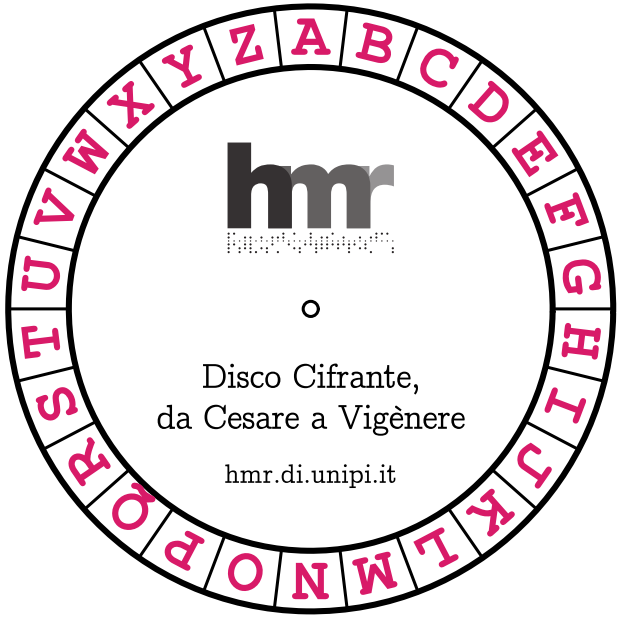

Disco Cifrante, da Cesare a Vigènere

La crittografia è una tecnica per nascondere un testo sostituendo le lettere secondo una regola nota solo a mittente e destinatario e, meglio ancora, dipendente da una chiave segreta. Il disco cifrante è uno strumento per giocare con alcuni metodi crittografici, come il cifrario di Cesare o quello di Vigènere.

Giulio Cesare, come racconta Svetonio, è stato uno dei primi a usare una tecnica crittografica. Per usare il disco cifrante al modo di Cesare occorre ruotarlo fino ad avere la D interna in corrispondenza alla A esterna. Poi, per cifrare si sostituiscono le lettere del testo leggendo il disco dall'esterno all'interno, viceversa per decifrare. Per esempio:

SONOARRIVATOALRUBICONEPORTATEMIIDADI
VRQRDUULYDWRDOUXELFRQHSRUWDWHPLLGDGL

Nel 1586 Blaise de Vigènere descrisse un altro metodo, più complicato, ma anche più sicuro. In precedenza altri avevano avuto idee simili, anche più sofisticate, ma il metodo di Vigènere ebbe più successo e fu ritenuto per molto tempo inviolabile.
Mittente e destinatario si accordano su una parola chiave, per esempio MISTERO, che viene giustapposta al testo ripetendola quante volte è necessario.
Per cifrare e decifrare si sostituiscono le lettere come per il cifrario di Cesare, ma a ogni lettera prima si ruota il disco facendo corrispondere la A esterna con la lettera interna data dalla corrente lettera della parola chiave. Per esempio:

VIGENEREINSUPERABILEINATTACABILEINOSSIDABILE
MISTEROMISTEROMISTEROMISTEROMISTEROMISTEROMI
HQYXRVFQQFLYGSDITBPVUZILMETONQDXMECEAAWESWXM

Museo degli Strumenti per il Calcolo

IN SUPREMÆ DIGNITATIS 1343

Giovanni A. Cignoni
hmr.di.unipi.it