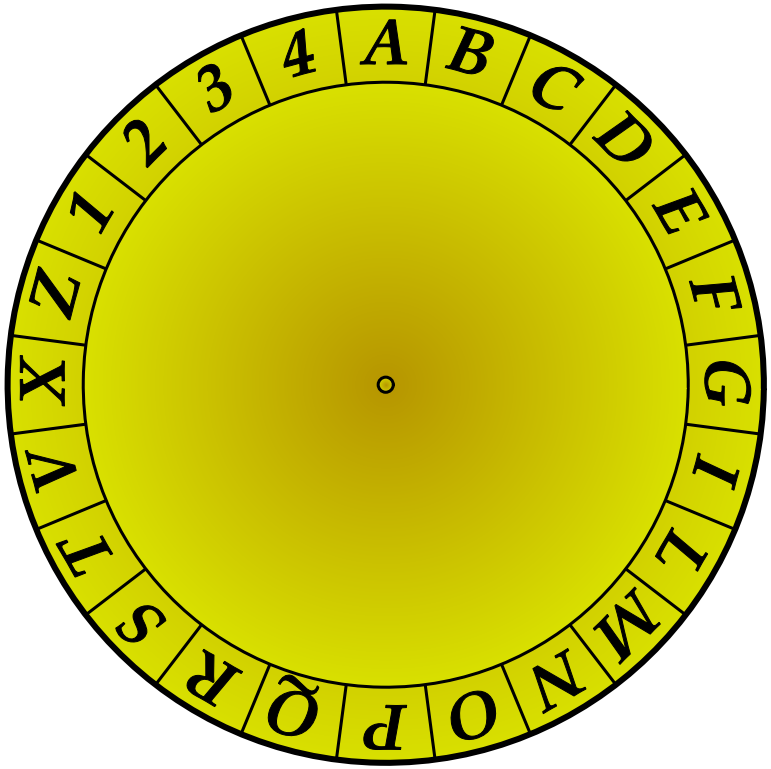

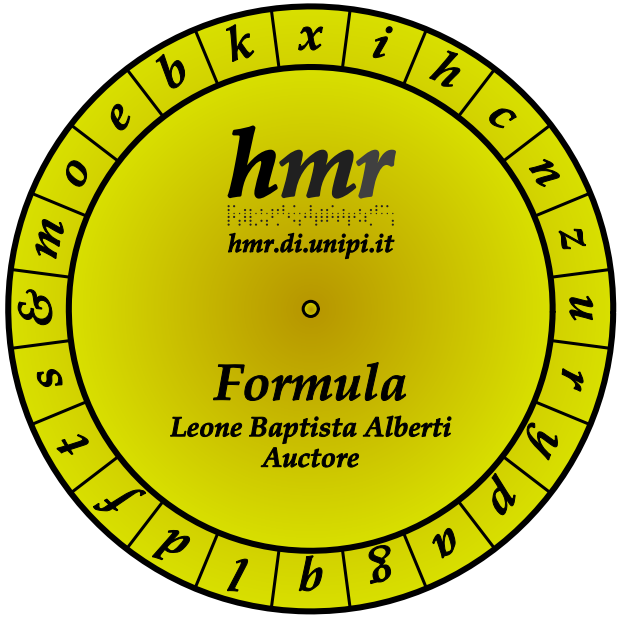

La *Formula* di Leon Battista Alberti

Leon Battista Alberti, architetto e umanista, scrisse nel 1466 il *De Componendis Cyfris*, un trattato di crittografia assai moderno per il suo tempo. Nei primi capitoli discute della frequenza delle lettere e delle sillabe come mezzi per attaccare un cifrario, poi propone un suo disco cifrante, la *Formula*, descrivendo alcuni metodi per usarlo. Vigènere, pur scrivendo oltre un secolo dopo, sembra non conoscere il lavoro dell'Alberti.

La Formula è composta di due dischi. Quello esterno è detto *stabilis*, riporta 24 simboli per il testo in chiaro, 20 lettere maiuscole (alcune rare e sostituibili sono sacrificate) e 4 cifre. Il disco interno, che Alberti chiama *mobilis*, riporta 24 simboli per il testo cifrato, 23 lettere minuscole e '&', allora già in uso come abbreviazione per "et". La Formula può essere usata in più modi, da semplici à la Cesare, a complessi con vocabolari di termini associati a valori numerici e cifrati usando le 4 cifre riportate sullo stabilis. Vi proponiamo il metodo polialfabetico descritto al capitolo XV del trattato.

Mittente e destinatario si accordano su un *index* scelto fra le maiuscole dello stabilis. Diciamo 'B'. Come prima lettera del cifrato si inserisce una minuscola a piacere, per esempio 'q'; è la lettera del mobilis da far corrispondere all'index per iniziare a cifrare. Ogni tanto si inserisce nel testo una delle 4 cifre dello stabilis: cifrata indica la nuova lettera del mobilis da far corrispondere all'index. Per esempio:

ALBE1RTI3MEGLI2ODIV1IGENE4REMEG3LIODI2CESARE
qgmqfroblnqrpgaxahutmixbnbsuoiobdeoxtoaglxpkl

Il metodo può essere variato introducendo vari accorgimenti per confondere eventuali curiosi. Alberti ne suggerisce alcuni, ma invita anche a inventarsene di propri. E così facciamo noi: buon divertimento!

Museo degli Strumenti per il Calcolo

Giovanni A. Cignoni
hmr.di.unipi.it