Schéma mental mathématique d'Enigma

N. Lygeros

P :=Permutation pour le clavier
U := Réflecteur
G :=Action du rotor de gauche
M :=Action du rotor du milieu
D :=Action du rotor de droite

ρ :=permutation circulaire
i :=nombre de positions à droite
j :=nombre de positions au milieu
k :=nombre de positions à gauche

CODAGE

$$C = PDMGUG^{-1}M^{-1}D^{-1}P^{-1}$$

CHIFFREMENT

$$C = P\left(\rho^{i}D\rho^{-i}\right)\left(\rho^{j}M\rho^{-j}\right)\left(\rho^{k}G\rho^{-k}\right)U\left(\rho^{k}G^{-1}\rho^{-k}\right)\left(\rho^{j}M^{-1}\rho^{-j}\right)\left(\rho^{i}D^{-1}\rho^{-i}\right)P^{-1}$$

PERIODE D'ENIGMA

$16900=26\times25\times26$ (3 rotors)