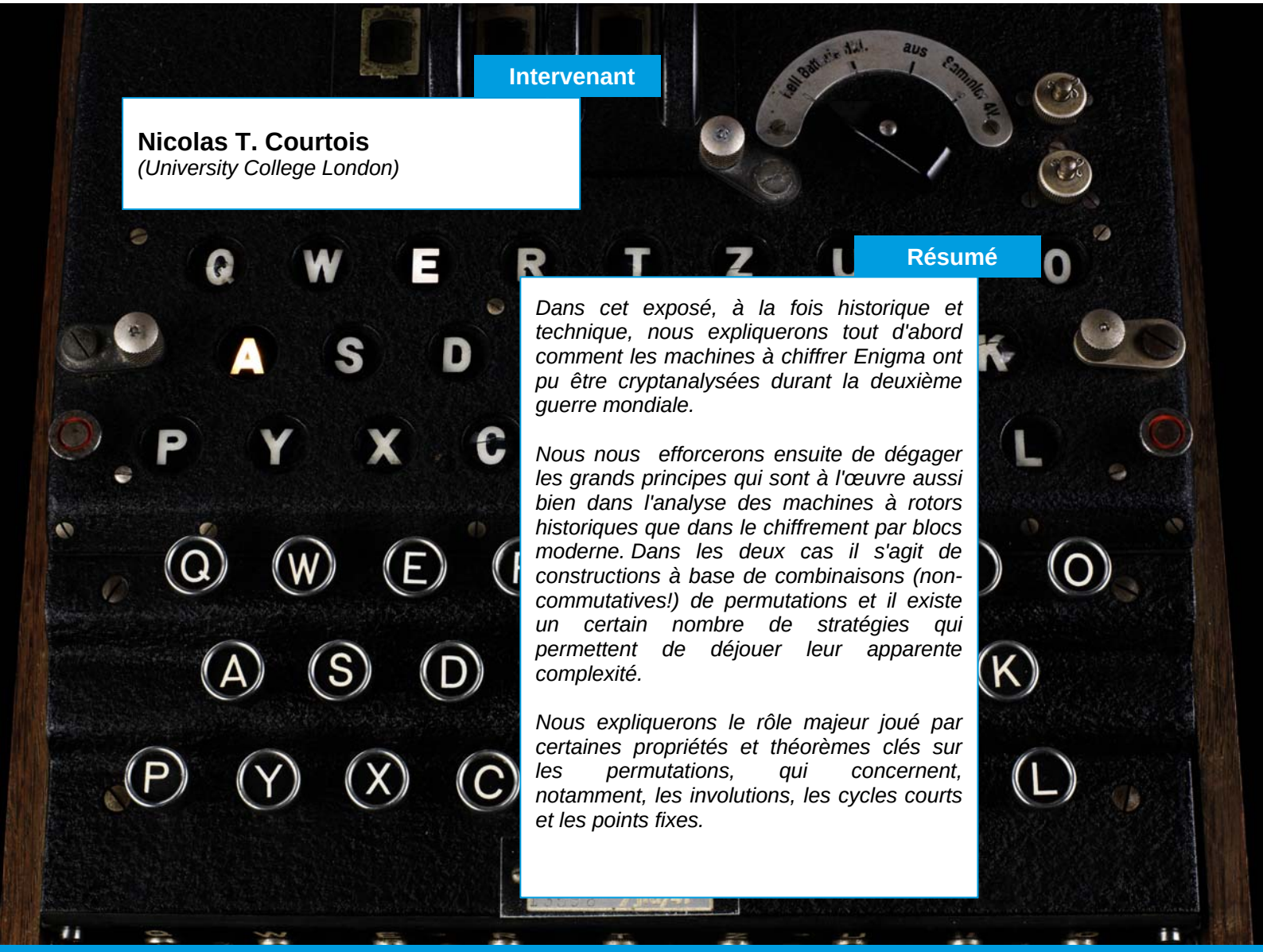
# Leçon de Mathématiques et d'Informatique d'Aujourd'hui

**Organisée par l'Ecole Doctorale de Mathématiques et d'Informatique**



**Intervenant**

**Nicolas T. Courtois**
*(University College London)*

**Résumé**

*Dans cet exposé, à la fois historique et technique, nous expliquerons tout d'abord comment les machines à chiffrer Enigma ont pu être cryptanalysées durant la deuxième guerre mondiale.*

*Nous nous efforcerons ensuite de dégager les grands principes qui sont à l'œuvre aussi bien dans l'analyse des machines à rotors historiques que dans le chiffrement par blocs moderne. Dans les deux cas il s'agit de constructions à base de combinaisons (non-commutatives!) de permutations et il existe un certain nombre de stratégies qui permettent de déjouer leur apparente complexité.*

*Nous expliquerons le rôle majeur joué par certaines propriétés et théorèmes clés sur les permutations, qui concernent, notamment, les involutions, les cycles courts et les points fixes.*

# Enigma, ou comment les mathématiciens ont gagné la guerre 1939-1945

## Jeudi 2 juin – 16h
## Amphithéâtre du LaBRI

**Infos : 05 40 00 87 07 – edmi@labri.fr**