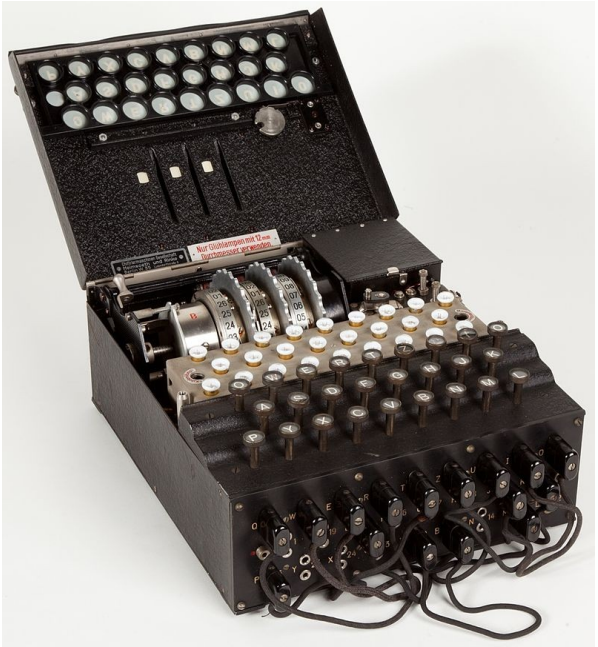
Matematika a tajemství Enigmy (Spoluorganizováno s ČMS)

Filip Soudský (TUL)

Na počátku dvacátého století se metody šifrování posunuly do nové éry. Dřívější ruční šifry byly nahrazeny strojovými šiframi. Nejslavnějším šifrovacím strojem první poloviny 20. století se stala Enigma, používaná zejména německými ozbrojenými složkami. Její úspěšné luštění hrálo významnou roli ve vývoji druhé světové války.



V dnešní přednášce se podíváme na to, jak šifra fungovala a zanalyzujeme způsoby, jakými se ji polským matematikům dařilo luštit. Podrobněji se zaměříme hlavně na metodu charakteristik, kterou se dařilo prolamovat denní klíče. Diskutované metody položily základ pozdějšímu britskému luštění v Bletchley parku.

Filip Soudský vystudoval matematickou analýzu na MFF UK se zaměřením na funkcionální analýzu a prostory funkcí. V současné době působí jako odborný asistent na katedře matematiky Fakulty přírodovědně humanitní a pedagogické Technické univerzity v Liberci.

Středa 18. prosince

17:30 v posluchárně K1

MFF UK, Sokolovská 49/83

nebo live stream na YouTube

MATEMATICKÉ PROBLÉMY NEMATEMATIKŮ

www.karlin.mff.cuni.cz/mffseminar najdete nás i na FB