Srdečně zveme všechny zájemce na kurz

pořádaný MFF UK v Praze v rámci

Univerzity třetího věku

v akademickém roce 2026/2027

Šifry v průběhu času

Lektor: Petr Brant

Kurz je jednosemestrální (zimní semestr), přednášky se budou konat ***online***

každý týden ve středu od 17 hodin

Zahájení ve **středu 14. října 2026**, všichni přihlášení budou mít možnost si od úterý 13.10. vyzkoušet spojení a funkce v MS Teams, pokud s tímto programem nemají zkušenost.

Odhalte tajemství skrytých zpráv od antiky po 2. světovou válku
Lákají vás záhady, historie a logické hádanky?
Přijďte si procvičit mozkové závity a nahlédnout do světa, kde informace měly cenu zlata a jejich utajení rozhodovalo o osudech říší.

Na co se můžete těšit?

- Jak komunikoval Julius Caesar nebo Marie Stuartovna?
- Jak šifroval kardinál Richelieu?
- Jak vypadá Vigenèrova šifra, kterou ale nevymyslel Vigenère?
- Co to je Polybiův čtverec? Ačkoliv je přes 2000 let starý, je základem mnoha šifer, třeba i těch, co používala Stasi nebo StB.
- Jaké šifry se používaly v americké občanské válce?
- Jak funguje šifra ADFGVX a proč má takový podivný název?
- Kdo vlastně vymyslel Enigmu a jak tento stroj funguje?
- Uvedeme na pravou míru některé scény z filmů o Enigmě
- Jak se šifrovalo po válce a jak se šifruje dnes?
- Existují dodnes nevyluštěné šifry?
- Existuje neprolomitelná šifra?
- Elektronický podpis a elektronická pečeť, certifikáty, šifrování s veřejným klíčem a mnoho dalšího
- Pro vážné zájemce je připravena výběrová přednáška, kde se bude rozebírat bezpečná výměna klíčů, princip Feistelovy sítě, šifry AES i RSA a vše, co s tím souvisí