Seminarium licencjackie dla MMAD

Kryptografia w teorii i praktyce

dr Iwona Krzyżanowska i dr Aleksandra Nowel

Nowoczesna kryptografia używa współczesnej matematyki, w szczególności teorii liczb, grup, pierścieni i ciał, algebry liniowej, prawdopodobieństwa i teorii informacji. Opiera się na algorytmach związanych z testowaniem pierwszości, faktoryzacją liczb całkowitych, dyskretnymi logarytmami i krzywymi eliptycznymi, dlatego przydaje się w niej także znajomość złożoności obliczeniowej, algorytmów i teorii zupełności NP. Na seminarium omówimy podstawowe rodzaje problemów badanych w kryptografii, jej cele oraz narzędzia i techniki w niej używane.

Literatura

1. Stinson, Douglas R.; Paterson, Maura B. *Kryptografia. W teorii i praktyce.* Wydawnictwo Naukowe PWN, 2021
2. Yan S.Y. *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN 2006
3. I.F. Blake, G. Seroussi and N.P. Smart *Elliptic Curves in Cryptography* London Mathematical Society Lecture Note Series Book 265
4. Neal Koblitz *A Course in Number Theory and Cryptography*
5. Thomas R. Shemanske *Modern Cryptography and Elliptic Curves: A Beginner's Guide*