Криптографија 2024./2025.

Мини курс Криптографије је први део специјалног курса, траје 4 седмице и представља увод у остале делове специјалног курса.

Док траје блокада основна литература су презентације. Окачено је укупно 8 презентација као замена за 4 предавања и 4 вежбе (при чему предавања и вежбе нису стриктно одвојени). У случају да нешто није јасно са презентација или желите да знате више литература је

- Neal Koblitz: *A course in number theory and criptography*, 2nd edition, Springer-Verlag, 1994.
- William Stein: *Elementary number theory: primes, conguences, and secrets*, 2017.
- Миодраг Живковић: *Криптографија*, 2020.

Испит се полаже писмено и обухвата све мини курсеве. На делу из криптографије долазе 3 кратка питања и 2 кратка задатка.

- Списак испитних питања
- Пример испита

На мом делу испита неће бити

- исписивање програмског кода,
- рачун са великим бројевима,
- математичко градиво (теорија бројева, алгебра) већ само примена истог на криптографију,
- упаривања на елиптичким кривама (последњи део мини курса). Упаривања вам требају за наредни мини курс Zero knowledge proofs, али за разумевање упаривања је потребно озбиљно математичко предзнање.

Имплементације алгоритама у пајтону можете наћи на страници Ивана Дрецуна

- https://github.com/idrecun/kripto-materijali