

Abstrakt algebra med konkrete anvendelser 2
Aalborg Universitet (2013)
Spiseseddel 12

12. gang, fredag d. 13. december, 17:00-20:00 i lokale G5-112

- Forelæsning: list dekodning (kapitel 12 fra [JH]). Offentlig-nøgle kryptografi: Knapsack, ElGamal, McEliece (Kapitel 8 fra [MOV]). Secret sharing (Afsnit 5.2 og 5.3 fra [GG])
- Opgaveregning: Gennemføre i Maple/Sage/Singular følgende kryptosystemer: Knapsack, ElGamal, McEliece.

Med venlig hilsen

Diego