KRYPTERING

- Historisk introduktion til kryptografiske systemer. (OTP)

  Gennem historien har mange gerne villet kunne skrive meddelelser, som kun kunne læses af en udvalgt skare. Vi fortæller om, hvordan det er blevet gjort gennem tiderne, og hvorfor det er mere aktuelt nu end nogensinde før. Herunder om symmetrisk og asymmetrisk kryptering og ideen bag public key systemer.

- Algebraen i public key systemer. (OTP)

  Public key systemer som f.eks. RSA bygger på ret simpel algebra samt at det er svært at primtalsfaktorisere. Vi vil fortælle om nogen af de metoder, der bruges. F.eks.:Modulær regning, One-way functions, primtalsalgoritmer, faktorisering, diskret logaritme.

- Opbygning og anvendelse af Public Key Systemer OTP.

  Deltagerne får selv lejlighed til at opbygge simple versioner af RSA-systemet, og vi fortæller om Knapsack, om ElGamal, om digital signatur og lidt videregående om mulighederne i kvantekryptering.