# Obligatorisk læringsaktivitet 2 i MAT102 - frist søndag 20/9

Denne innleveringen er den andre obligatoriske læringsktiviteten i MAT102. Innleveringen skal bestå av en fil: kjørbar kodefil som svarer på oppgavene om RSA. Svar på oppgavene skal være en del av filen som kommentarer. Sett også inn resultatet av kjøring som kommentar.

Dere har lov til å bruke alle funksjonsfilene jeg har delt med dere direkte, og disse filene skal ikke være en del av innleveringen. Det betyr for eksempel at dere kan kalle powerMod-funksjonen i filen dere levererer. NB: Ikke gjør noen endringer i disse filene! Vi skal kunne kjøre den leverte filen ved å kalle de originale filene.

- Svar på oppgaver som ikke forventes løst av programmet skal stå som kommentar i besvarelsen. Eksempel:

  ```
  %a: Den dekodede beskjeden blir ...
  ```

- Svar på oppgaver som skal løses av programmet skal stå under koden som gir svaret, som kommentar. Eksempel:

  ```
  %c: Kode for å kryptere HEI SJEF:
  ... Koden dere skriver
  % Svaret når koden kjøres er: ...
  ```

Lever i grupper på tre, maksimalt fire. På grunn av corona-situasjonen anbefaler vi å bruke samme grupper i alle fag i den grad det er praktisk gjenomførbart.

Hvis noen vil besvare oppgaven ved å bruke Python: Det er lov, men dere må regne med noe ekstra egenarbeid siden presentasjonen av stoffet i kurset i hovedsak har fulgt Matlab. Filen RSA.py, som dere finner i modulen *For de spesielt interesserte: Litt om Python for vårt kurs*, inneholder de ulike hjelpefunksjonene skrevet i Python. Etter at denne filen kjøres er funksjonene tilgjengelig i minnet, og filen dere leverer skal så være kjørbar.

# RSA-oppgave

I et oppsett for RSA er den offentlige nøkkelen $(n, e)$ gitt ved

$$n = 104523733 \quad \text{og} \quad e = 137.$$

For å sende beskjeder kodes en tekststreng (i engelsk alfabet, uten æøå) ved $A \leftrightarrow 00, B \leftrightarrow 01, \ldots, Z \leftrightarrow 25$. I tillegg lar vi mellomrom være representert ved 99. Strengen deles opp i fire og fire tegn. Hvert firetuppel er dermed representert som et tall mellom 0 (AAAA) og 99999999 (fire mellomrom).

a) En kodet beskjed har representasjonen $[1041706, 4139999]$. Dekod beskjeden.

b) Kod meldingen `HEI SJEF`.

c) Krypter meldingen `HEI SJEF`.

Vi skal så knekke dette oppsettet, og finne ut hva den hemmelige beskjeden $U$ vi har snappet opp betyr:

$$U = [16646055, 76586540, 40429350, 81029513, 98012653, 6683466]$$

d) Finn primtallene $p$ og $q$ slik at $n = pq$.

e) Hva må til for at $(n, e)$ skal være en korrekt valgt nøkkel for RSA? Sjekk dette for den oppgitte nøkkelen $(n, e)$.

f) Regn ut dekrypteringsnøkkelen $(n, d)$. Kontroller svaret ved å dekryptere resultatet fra deloppgave c).

g) Dekrypter og dekod den hemmelige beskjeden $U$.

# Til slutt

Ikke glem å spørre om hjelp på regneøvelser eller i forbindelse med forelesninger. Dette er ikke en eksamen, men en obligatorisk oppgave som det er meningen dere skal lære av å arbeide med.

Lykke til!

Preben og Jon Eivind