Institut for Matematik og Datalogi
Syddansk Universitet

Afleveringsopgave 6 — DM534 efterår 2014

Dette er sjette (og sidste) afleveringsopgave i DM534. Deadline er

Torsdag den 18. december, 2014, kl. 08:15.

Opgaven skal skrives i LaTeX, men du behøver ikke at inkludere LaTeX-koden. Du kan skrive på dansk eller på engelsk. Skriv dit navn, holdnummer og navnet på din instruktor (Magnus Gausdal Find eller Christian Kudahl) på første side af afleveringen.

Du skal aflevere én pdf-fil via "SDU Assignment" på Blackboard-siden for DM534. Husk at aflevere under det korrekte holdnummer og at gemme kvitteringen. Bemærk at Blackboard lukker for afleveringen ved udløb af deadline.

Opgaven udgør en del af eksamen i DM534, så samarbejde om at udarbejde besvarelsen, kopiering fra medstuderende, internettet eller andre steder, samt andre former for brug af andres indsats er derfor eksamenssnyd. Du må til gengæld gerne referere til og bruge stof fra lærebog og slides. Hvis du har spørgsmål til opgaven, så kontakt Joan Boyar, Rolf Fagerberg eller din instruktor i DM534.

Opgaven skal godkendes for at du kan bestå DM534. Hvis du ikke får din første aflevering af den godkendt, eller ikke får den afleveret til deadline, vil den tælle som én af de i alt to genafleveringer, du kan lave i DM534. Din genaflevering af opgaven skal så godkendes i første forsøg.

Afleveringsopgave 6

Løs alle nedenstående opgaver. Besvarelserne skal være klare og fuldstændige, men ikke længere end nødvendigt. Gentag ikke problemformuleringer, og giv ikke informationer, som der ikke bedes om.

1. Denne opgave handler om kryptering med RSA-metoden. Brug notation og algoritmer fra slides fra forelæsningerne om kryptologi (kan

findes på kursets webside). Du kan godt bruge f.eks. Maple til at checke dine beregninger, men du skal alligevel beskrive alle skridt i udregningerne i algoritmerne, som krævet nedenfor.

Lad de offentlige nøgler være $N_A = 1363$ og $e_A = 13$.

(a) Kryptér beskeden $m = 213$. Til modulær potensopløftning skal du bruge algoritmen fra side 30 af slides. (Du kan også bruge varianten vist til øvelsestimerne, men angiv så at du bruger denne.) Vis alle skridt i udregningerne.

(b) Det oplyses at $p = 29$ og $q = 47$ (hvis du selv havde lavet de offentlige nøgler, ville du som bekendt være startet med at vælge p og q). Fra denne information, samt $e_A = 13$, beregn den hemmelige nøgle d_A. Brug Extended Euclidian Algorithm fra side 48 af slides (du kan også bruge varianten vist til øvelsestimerne, men angiv så at du bruger denne). Vis alle skridt i udregningerne.

(c) Dekryptér den krypterede besked fra første del. Brug den samme algoritme til modulær potensopløftning som før, og vis alle skridt i udregningerne.

2. Lav problem 28 på side 518 i lærebogen. Det er OK at lave en håndtegning, som scannes og inkluderes i LaTeX-dokumentet.

3. Lav problem 46 på side 520 i lærebogen. For at lette rettearbejdet skal du lave i alt fem tegninger af dit netværk:

   - Én som figur 11.18, hvor du viser vægte (w_i'erne) og thresholds for alle knuderne i dit netværk.
   - I alt fire figurer, en for hvert af de mulige input 00, 01, 10, 11, hvor du viser værdierne på kanterne (v_i'erne) i netværket for dette input.

   Det er OK at lave håndtegninger, som scannes og inkluderes i LaTeX-dokumentet.