Institut for Matematik og Datalogi
Syddansk Universitet, Odense

4. marts 2013
RF

Afleveringsopgave 6
DM534 efterår 2012/forår 2013

Opgaver

I det følgende betragtes et RSA-system med $n = 1517$ og krypteringsnøgle $e = 227$.

1. Krypter beskeden 423. Til eksponentiering skal bruges algoritmen fra side 2 i noterne om de algoritmiske aspekter af RSA. Vis alle beregninger undervejs.

2. Det afsløres at $N = (p-1)(q-1)$ er lig 1440. Find dekrypteringsnøglen d – dvs. find tallet d, så $de = 1 \pmod{N}$. Dette skal gøres ved at bruge Euklids udvidede algoritme, som forklaret sidst på side 3 i noterne om de algoritmiske aspekter af RSA. Vis alle beregningerne undervejs i algoritmen.

3. Dekrypter din besked igen. Vis alle beregninger undervejs i brugen af algoritmen fra side 2 i noterne.

Formalia

Din besvarelse skal starte med dit *fulde navn* og *holdnummer* (S7/S17).

Du skal bruge LaTeX til at indskrive besvarelsen. Du skal blot aflevere besvarelsen af ovenstående spørgsmål, *ikke* filen med LaTeX-kildeteksten.

Du skal både aflevere på papir (for at få rettelser tilbage) og elektronisk (for at vi kan overholde arkiveringskrav, og for at du kan få en kvittering for aflevering). De to afleveringer skal være ens. Den elektroniske version skal være et pdf-dokument.

Aflevering på papir sker i instruktorens dueslag. Instruktoren er for begge hold Rojin Kianian, som har dueslag overfor fagrådslokalet på Imada. Aflevering elektronisk sker i Blackboard med værktøjet "SDU Assignment". Det kan findes i menuen på kursets side i Blackboard. Menuen findes ved at klikke på det lille "dobbelt-firkant"-ikon i øverste halvdel af venstre kant af kursets side i Blackboard (om nødvendigt maksimer det fremkomne vindue).

Opgaven er en del af den individuelle eksamen i DM534, så samarbejde om at udarbejde besvarelser, og kopiering af indhold fra WWW eller andre steder, er derfor at betragte som eksamenssnyd. Du må gerne stille spørgsmål om opgaven til instruktor og underviser. Bestået af eksamen i DM534 kræver godkendelse af alle seks afleveringsopgaver. Op til to af disse må blive genafleveret efter ikke at være blevet godkendt.

Afleveringsfristen skal overholdes for at blive godkendt. Blackboard lukker for aflevering ved fristens udløb. Det anbefales stærkt at man planlægger at aflevere dagen før deadline.

Afleveringsfristen er:

Fredag den 22. marts, 2013, kl. 12:00.