Institut for Matematik og Datalogi
Syddansk Universitet, Odense

1. marts 2013
RF

Eksaminatorier DM534

Uge 10

I de to første opgaver nedenfor kan det være brugbart at kende, hvor hyppigt de enkelte bogstaver forekommer i gennemsnit i Engelsk tekst. Dette kan ses f.eks. på Wikipedia under opslaget Letter frequency.

1. Følgende besked (på engelsk, dvs. alfabetstørrelse 26) er blevet krypteret med en Cæsar-kode, dvs. hvor hvert bogstav er blevet erstattet ved et cyklisk skift af alfabetet (se evt. side 208 i bogen fra DM535 Diskrete Metoder til Datalogi). Mellemrum og punktuation er ikke ændret.

   YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

   Forsøg at dekryptere beskeden.

2. Følgende besked (på engelsk, dvs. alfabetstørrelse 26) er blevet krypteret med en generel substitutionskode, dvs. hvor hvert bogstav i alfabetet er blevet erstattet med et andet (alfabetet er permuteret). Mellemrum og punktuation er ikke ændret.

   TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC.
   UFYR FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB
   BWWR CWWD.

   Forsøg at dekryptere beskeden.

3. I noterne om de algoritmiske aspekter af RSA er angivet en rekursiv algoritme til at beregne $x^k \pmod{n}$. Implementer denne i enten Java (med datatypen `long`), eller Python. Den skal modtage x, k og n som argumenter, og skal returnere $x^k \pmod{n}$ beregnet ved hjælp af algoritmen på side 2 i noterne.

4. Chapter Review Problems 48, side 557. Håndkør algoritmen fra side 2 i noterne, og vis de beregnede tal undervejs. Check svaret med din implementation. Bemærk at beskeden er angivet som en bitstreng, og skal fortolkes som et (binært) heltal før det kan krypteres.

5. Chapter Review Problems 50, side 557. Du skal her først gætte, hvad p og q er i $n = pq$ (det er dette skridt, som forventes ikke at kunne gøres effektivt for store n (såsom tal med 1024 bits)). Dernæst skal du finde d, så $de = 1 \pmod{N}$ for $N = (p-1)(q-1)$. Dette kan gøres enten ved at gætte og teste (da tallene er små), eller ved at køre Euklids udvidede algoritme, som forklaret sidst på side 3 i noterne om de algoritmiske aspekter af RSA.

6. I det følgende betragtes et RSA-system med $n = 17399$ og krypteringsnøgle $e = 5$.

   (a) Krypter beskeden 16410. Vis alle beregninger undervejs i brugen af algoritmen fra side 2 i noterne.

   (b) Det afsløres at $N = (p-1)(q-1)$ er lig 17136. 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.

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

7. I det følgende betragtes et RSA-system med $n = 11413$ og krypteringsnøgle $e = 3533$.

   (a) Krypter beskeden 9726. Vis alle beregninger undervejs i brugen af algoritmen fra side 2 i noterne.

   (b) Det afsløres at $N = (p-1)(q-1)$ er lig 11200. 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.

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