KRYPTOGRAFIAN ALKEET

2. RÄKNEÖVNINGEN

I de första uppgifterna är idén att bekanta sig med DES-algoritmen, medan man i de sista uppgifterna skall repetera grunder i talteori som behövs i fortsättningen av kursen.

Det finns en hel del material om talteori på nätet. En möjlighet är att använda materialet från kursen Elementär talteori från våren 2013. Hemsidan hittas på

`http://wiki.helsinki.fi/pages/viewpage.action?pageId=96704243`

(1) Låt

$w =$ 00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111.

Detta skall krypteras med DES-algoritmen. Utför den första permutationen och indelningen i blocken L_0 och R_0.

(2) Låt DES-algoritmens hemliga nyckel vara

$$K = 000100100011010001010110011111000100110101011110011011110.$$

Beräkna kontrollbitarna. Bestäm därtill blocken C_0, D_0, C_1, D_1, skapa med hjälp av dem nyckeln K_1 och använd nyckeln för att beräkna blocken L_1 och R_1.

(3) När existerar det en lösning till en diofantisk ekvation av första graden med två variabler? Lös den diofantiska ekvationen

$$8x + 5y = 3$$

(4) Påminn dig om vad Fermats lilla sats säger. Beräkna $3^{58} \pmod{59}$.

(5) Vad är en primitiv rot? Vad betyder begreppet ordning? Bestäm alla primitiva rötter modulo 7 och ordningen för alla element i det reducerade restsystemet.

(6) Vad är Eulers φ-funktion? Beräkna

$$\varphi(29),\ \varphi(30),\ \varphi(16).$$

(7) Vad säger Eulers sats? Beräkna $7^{25} \pmod{30}$.