TATA32-ETE373: Inlämninguppgifter 2024, Del 2 Enigma-maskinen

Lämnas in senast 21/10 2024, kl.13.00

Caesar-Kryptering för svenska alfabetet

Givet alfabetet $\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z,$ Å, Ä, Ö $\}$, identifierar vi A med 1, B med 2, C med 3, D med 4, E med 5, F med 6, G med 7, H med 8, I med 9, J med 10, K med 11, L med 12, M med 13, N med 14, O med 15, P med 16, Q med 17, R med 18, S med 19, T med 20, U med 21, V med 22, W med 23, X med 24, Y med 25, Z med 26, Å med 27, Ä med 28 och Ö med 29. Så $\mathcal{A}$ identifieras med $\mathbb{Z}_{29}$. Ceasar-kryptering på alfabetet är en avbildning $s_c : \mathbb{Z}_{29} \to \mathbb{Z}_{29}, 1 \leq c \leq 28$ så att till varje element $x \in \mathbb{Z}_{29}$ tilldelas $s_c(x) \equiv x + c$ mod29. Det vill säga man avancerar cykliskt c bokstäver i alfabetet, observera att mellanrum mellan ord flyttas inte utan är fortfarande mellanrum. Avkrypteringsprocedur $d_c : \mathbb{Z}_{29} \to \mathbb{Z}_{29}, 1 \leq c \leq 28$ är att subtrahera c (cykliskt): $d_c(x) \equiv x - c$ mod29.

Fråga 1 Visa att s_c och d_c är bra krypterings- och avkrypteringsavbildningar.

Enigma-maskinen

Enigma-maskinen användes av tyskarna under WWII för att kryptera meddelanden med Ceasar-kryptering. Maskinen som användes vid slutet av kriget består av fem rotorer. Varje rotor består av 28 positioner, där varje position ger hur många bokstäver vi avancerar i alfabetet med Caesar-krypteringen ovan. För att kryptera ett meddelande delade man in varje meddelande i block med 5 symboler. Första symbol i varje block avancerar, om den är en bokstvav och inte ett mellanrum, så många steg som rotor 1 säger, andra symbol i varje block avancerar så många steg som rotor 2 säger, osv (sista blocket kan innehålla 1 till 5 symboler). Krypteringen ändrades varje dag.

Fråga 2 På hur många olika sätt kan man kryptera ett meddelande. Svara med heltal.

Egen kryptering

För dagens kryptering antag nu att rotorer har positioner som beror på era parametrar som följer:

1. Position i Rotor 1 ges av antal bokstäver i ert förnamn.
2. Position i Rotor 2 ges av antal bokstäver i ert efternamn.
3. Position i Rotor 3 ges av $c_3 = d_1 + d_2 + m_1 + m_2$, där d_1, d_2, m_1, m_2 är som i ditt födelsedatum $d_1d_2 - m_1m_2 - 20x_1x_2$ eller $d_1d_2 - m_1m_2 - 19x_1x_2$.
4. Position i Rotor 4 ges av $c_4 = x_1 + x_2 + 9$ där x_1, x_2 är som i ditt födelsedatum.
5. Position i Rotor 5 ges av $c_5 = m_2 + d_2 + 3$ där m_2, d_2 är som i ditt födelsedatum.

Fråga 3 Kryptera med dina parametrar 'HEJ VÄLKOMMEN TILL DISKRET MATEMATIK' (36 symboler)

Fråga 4 Avkryptera 'PNS CGUTDWUNW AQUU NQÄTGOÄ VSAMVJISS ' (36 symboler). Observera att det inte är krypterat med era parametrar, utan ni måste komma på rotorpositionerna; ange dem och resonera.