ENCRYPTION

Take 6 Plain Text

$P_1 = 65535$ $P_2 = 38459$ $P_3 = 14632$

$P_4 = 18591$ $P_5 = 55321$ $P_6 = 81321$

$$M = \prod_{i=1}^{6} m_i \Rightarrow (41 \times 43 \times 45 \times 47 \times 49 \times 53)$$

$M = 9683550765$

$$M_i = \frac{M}{m_i}$$

step 1

$M_1 = \frac{9683550765}{41} = 236184165$

$M_2 = \frac{M}{43} = 225198855$

$M_3 = \frac{M}{45} = 215190017$

$M_4 = \frac{M}{47} = 206032995$

$M_5 = \frac{M}{49} = 197623485$

$M_6 = \frac{M}{53} = 182708505$

$$X_i = (m_i \times m_i^{-1}) \bmod M_i \equiv 1$$

$X_1 = (M_1 \times m_1^{-1}) \bmod M_1 \equiv 1 \Rightarrow 132493556$

$X_2 = (m_2 \times m_2^{-1}) \bmod M_2 \equiv 1 \Rightarrow 209487307$

$X_3 = (m_3 \times m_3^{-1}) \bmod M_3 \equiv 1 \Rightarrow 176934014$

$X_4 = (m_4 \times m_4^{-1}) \bmod M_4 \equiv 1 \Rightarrow 175347123$

$X_5 = (m_5 \times m_5^{-1}) \bmod M_5 \equiv 1 \Rightarrow 92762044$

$X_6 = (m_6 \times m_6^{-1}) \bmod M_6 \equiv 1 \Rightarrow 24131312$

$x_i = P_i \times X_i \bmod M_i$

$x_1 = 65535 \times 132493556 \bmod 236184165 = 126734565$

$x_2 = 38459 \times 209487307 \bmod 225198855 = 183302288$

$x_3 = 14632 \times 176934074 \bmod 215190017 = 162588338$

$x_4 = 18591 \times 175347123 \bmod 206032995 = 43837203$

$x_5 = 55321 \times 92762044 \bmod 197623485 = 1129$

$x_6 = 81321 \times 24131312 \bmod 182708505 = 93079452$

$C_i = x_i \times K \bmod M_i$ where $K \times K^1 \bmod r_i = 1$

assume $K = 58$

$C_1 = 126734565 \times 58 \bmod 236184165$

$= 28895655$

$K^1 = 36649267$

$C_2 = 183302288 \times 58 \bmod 225198855$

$= 47186519$

$K^1 = 91068472$

$C_3 = 162588338 \times 58 \bmod 215190017$

$= 176952873$

$K^1 = 152117081$

$C_4 = 43837203^{58} \bmod 206032995$

$= 70161834$

$K^1 = 202480702$

$C_5 = 1129 \times 58 \bmod 197623485$

$= 65482$

$K^1 = 51109522$

$C_6 = 93079452 \times 58 \bmod 182708505$

$= 100061571$

$K^1 = 148056992$

Send $C_1, C_2, C_3, C_4, C_5, C_6$

Send to skipjack encryptor

DECRYPTION

Decrypt $C_1, C_2, C_3, C_4, C_5, C_6 \Rightarrow P_1, P_2, P_3, P_4, P_5$

$C_1 = 28895655$ $C_2 = 4718.6519$ $C_3 = 176952873$

$C_4 = 70161834$ $C_5 = 65482$ $C_6 = 100061571$

$x_i = (C_i \times K_i^{-1}) \bmod M_i$ where $K^{-1} \Rightarrow K \times K_i^{-1} \bmod M_i$

Here $K = 58$

$x_1 = 28895655 \times 36649267 \bmod 236184165$

(C_1, K_i^{-1})

$x_1 = 126734565$

$x_2 = 4718.6519 \times 97068472 \bmod 225198855$

$x_2 = 118330288$

$x_3 = 176952873 \times 152117081 \bmod 215190017$

$= 162588338$

$x_4 = 70161834 \times 202480702 \bmod 206032995$

$= 43837203$

$x_5 = 65482 \times 51109522 \bmod 197623485$

$= 1129$

$x_6 = 100061571 \times 148056892 \bmod 182708505$

$= 93079452$

$P_i = x_i \times m_i \bmod M_i$

$P_1 = 126736565 \times 41 \bmod 236184165 = 65535$

$P_2 = 183302288 \times 43 \bmod 225198855 = 38459$

$P_3 = 162588338 \times 45 \bmod 215190017 = 14632$

$P_4 = 43857203 \times 47 \bmod 206032995 = 18591$

$P_5 = 1129 \times 49 \bmod 197623485 = 55321$

$P_6 = 93079482 \times 53 \bmod 182703505 = 81321$