Diffie Hellman Key Exchange Algorithm

For user A and B exchange the key using Diffie Hellman algorithm. Assume $\alpha=3$, $q=353$, $x_a=97$, $x_b=233$, now find the value of y_a, y_b and k.

Solution:

Now we calculate public of user A

- $y_A = \alpha^{xA} \bmod q$

$= (3)^{97} \bmod 353$

$=3^* 3^{96} \bmod 353= 3^*(3^2)^{48} \bmod 353= 3^* (3^2 \bmod 353)^{48} \bmod 353$

$=3^* (9)^{48} \bmod 353= 3^* (9^2)^{24} \bmod 353= 3^* (81 \bmod 353)^{24} \bmod 353$

$=3^* (81)^{24} \bmod 353 = 3^* (81^2)^{12} \bmod 353$

$=3^* (6561 \bmod 353)^{12} \bmod 353$

$= 3^* 207^{12} \bmod 353$

$= 3^* (207^2 \bmod 353)^6 \bmod 353$

$= 3^* 136^6 \bmod 353$

$=3^* (136^2 \bmod 353)^3 \bmod 353$

$=3^* 140^3 \bmod 353$

$=3^* (140^* (140^2 \bmod 353) \bmod 353) \bmod 353$

$=3^* (140^*185 \bmod 353) \bmod 353$

$=3^* (25900 \bmod 353) \bmod 353$

$=40$

Now we calculate public of user B

- $y_B = \alpha^{xB} \bmod q$

$=3^{233} \bmod 353$

$= 3* 3^{232} \bmod 353 = 3* (3^2 \bmod 353)^{116} \bmod 353$

$=3* 9^{116} \bmod 353 = 3* (9^2 \bmod 353)^{58} \bmod 353$

$=3* 81^{58} \bmod 353$

$=3* (81^2 \bmod 353)^{29} \bmod 353$

$=3* 207^{29} \bmod 353$

$= 3* (207* 207^{28} \bmod 353) \bmod 353$

$=3* (207 (207^2 \bmod 353)^{14} \bmod 353) \bmod 353$

$=3* (207* 136^{14} \bmod 353) \bmod 353$

$=3* (207* (136^2 \bmod 353)^7 \bmod 353) \bmod 353$

$=3* (207* 140^7 \bmod 353) \bmod 353$

$=3* (207 * [140* 140^6] \bmod 353) \bmod 353$

$=3*(207* [140* (140^2 \bmod 353)^3 \bmod 353] \bmod 353$

$=3*(207* [140* 185^3 \bmod 353] \bmod 353) \bmod 353$

$=3*(207 * [140* (185* (185^2 \bmod 353) \bmod 353) \bmod 353] \bmod 353$

$=3*(207* [140* (185* 337 \bmod 353) \bmod 353] \bmod 353$

$=3* (207*[140* 217 \bmod 353] \bmod 353) \bmod 353$

$=3* (207 *22 \bmod 353) \bmod 353$

$=3* 318 \bmod 353 = 954 \bmod 353$

$=248$

Now Common Secret key of A

$K_{AB} = y_B^{xA} \bmod 353$

$=248^{97} \bmod 353$

$=248 * (248^2 \bmod 353)^{48} \bmod 353$

$=248 * (82)^{48} \bmod 353$

$=248 * (82^2 \bmod 353)^{24} \bmod 353$

$=248 * (17)^{24} \bmod 353$

$=248 * (17^2 \bmod 353)^{12} \bmod 353$

$=248 * 289^{12} \bmod 353$

$=248 * (289^2 \bmod 353)^{6} \bmod 353$

$=248 * (213)^{6} \bmod 353$

$=248 * (213^2 \bmod 353)^{3} \bmod 353$

$=248 * (185)^{3} \bmod 353$

$=248 * (185*(185^2 \bmod 353) \bmod 353) \bmod 353$

$=248 * (185* 337 \bmod 353) \bmod 353$

$=248 * 217 \bmod 353 = 53816 \bmod 353$

$= 160$

Now Common Secret key of B

$K_{AB} = y_A^{xB} \bmod 353$

$=40^{233} \bmod 353$

$= 40* 40^{232} \bmod 353$

$=40* (40^2 \bmod 353)^{116} \bmod 353$

$=40* (188)^{116} \bmod 353$

$=40* (188^2 \bmod 353)^{58} \bmod 353$

$=40* 44^{58} \bmod 353$

$=40* (44^2 \bmod 353)^{29} \bmod 353$

$=40 * (171)^{29} \bmod 353$

$=40* (171* 171^{28} \bmod 353) \bmod 353$

$=40 * (171* (171^2 \bmod 353)^{14} \bmod 353) \bmod 353$

$=40* (171* 295^{14} \bmod 353) \bmod 353$

$=40 * (171* [295^2 \bmod 353]^7 \bmod 353$

$=40* (171* [187^7] \bmod 353) \bmod 353$

$=40* (171* [187* 187^6 \bmod 353] \bmod 353) \bmod 353$

$=40* (171*[187* \{187^2 \bmod 353\}^3 \bmod 353] \bmod 353) \bmod 353$

$=40 * (171*[187* 22^3 \bmod 353] \bmod 353) \bmod 353$

$=40 * (171* [187* \{22* (22^2 \bmod 353) \bmod 353\} \bmod 353] \bmod 353) \bmod 353$

$=40 * (171* [187* \{22*131 \bmod 353\} \bmod 353] \bmod 353) \bmod 353$

$=40*(171* [187*58 \bmod 353] \bmod 353) \bmod 353$

$=40* (171* 256 \bmod 353) \bmod 353$

$=40* 4 \bmod 353$

$=160 \bmod 353$

$=160$