

RSA Algorithm

Find the ciphertext and corresponding plaintext of given following

Given prime Number $p=17$, $q=11$, Plaintext, $M=88$

$$N=p*q=17*11=187$$

$$\begin{aligned}\phi(n) &= (p-1)(q-1) \\ &= 16*10=160\end{aligned}$$

e =public key

$$\gcd(\phi(n), e)$$

for $e=2$, $\gcd(160,2)$

for $e=3$, $\gcd(160,3)=1$; remainder exist

now public key $e=3$

$$\text{now } d = (1 + \phi(n) \cdot k) / e$$

$$\text{when } k=0, d = (1 + 160 \cdot 0) / 3 = 1/3;$$

$$k=1, d = (1 + 160 \cdot 1) / 3 = 161/3;$$

$$k=2, d = (1 + 160 \cdot 2) / 3 = 321/3 = 107$$

private key $d=107$

we have $e=3$, $d=107$, $n=187$

public key = $(3, 187)$

private key= (107, 187)

plaintext M=88

$$C=M^e \text{ mod } n$$

$$=88^3 \text{ mod } 187$$

$$=88*88^2 \text{ mod } 187$$

$$=88(7744 \text{ mod } 187)\text{mod } 187$$

$$=88*77 \text{ mod } 187$$

$$= 6776 \text{ mod } 187$$

$$=44$$

Ciphertext C=44

$$M=C^d \text{ mod } n$$

$$=44^{107} \text{ mod } 187$$

$$= 44* 44^{106} \text{ mod } 187$$

$$=44* (44^2)^{53} \text{ mod } 187$$

$$=44* (1936 \text{ mod } 187)^{53} \text{ mod } 187$$

$$=44* (66)^{53} \text{ mod } 187$$

$$=44* \{66* 66^{52} \text{ mod } 187\} \text{ mod } 187$$

$$=44* \{66* (66^2)^{26} \text{ mod } 187\} \text{ mod } 187$$

$$=44* \{66* (4356 \text{ mod } 187)^{26} \text{ mod } 187\} \text{ mod } 187$$

$$\begin{aligned}
&=44* \{66*55^{26} \bmod 187\} \bmod 187 \\
&=44* \{66*(55^2)^{13} \bmod 187\} \bmod 187 \\
&=44* \{66* (3025 \bmod 187)^{13} \bmod 187\} \bmod 187 \\
&=44* \{66* 33^{13} \bmod 187\} \bmod 187 \\
&=44* \{66* (33*[33^{12} \bmod 187] \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* (33^2)^6 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* [1089 \bmod 187]^6 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33*154^6 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* (154^2)^3 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* (23716 \bmod 187)^3 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* 154^3 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* [154* 154^2 \bmod 187] \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* [154* (23716 \bmod 187) \bmod 187] \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33* [154*154 \bmod 187] \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33*[23716 \bmod 187] \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (33*154 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66* (5083 \bmod 187) \bmod 187\} \bmod 187 \\
&=44* \{66*33 \bmod 187\} \bmod 187 \\
&=44* \{2178 \bmod 187\} \bmod 187
\end{aligned}$$

$$=44 * 121 \bmod 187$$

$$=5324 \bmod 187$$

$$=88$$

Plaintext M=88

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

$$\bullet y_A = \alpha^{x_A} \text{ mod } q$$

$$= (3)^{97} \text{ mod } 353$$

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

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

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

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

$$= 3 * 207^{12} \text{ mod } 353$$

$$= 3 * (207^2 \text{ mod } 353)^6 \text{ mod } 353$$

$$= 3 * 136^6 \text{ mod } 353$$

$$= 3 * (136^2 \text{ mod } 353)^3 \text{ mod } 353$$

$$= 3 * 140^3 \text{ mod } 353$$

$$= 3 * (140 * (140^2 \text{ mod } 353) \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (140 * 185 \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (25900 \text{ mod } 353) \text{ mod } 353$$

$$= 40$$

Now we calculate public of user B

$$\bullet y_B = \alpha^{xB} \text{ mod } q$$

$$= 3^{233} \text{ mod } 353$$

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

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

$$= 3 * 81^{58} \text{ mod } 353$$

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

$$= 3 * 207^{29} \text{ mod } 353$$

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

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

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

$$= 3 * (207 * (136^2 \text{ mod } 353)^7 \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * 140^7 \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * 140^6] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * (140^2 \text{ mod } 353)^3 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * 185^3 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * (185 * (185^2 \text{ mod } 353) \text{ mod } 353) \text{ mod } 353] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * (185 * 337 \text{ mod } 353) \text{ mod } 353] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * [140 * 217 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353$$

$$= 3 * (207 * 22 \text{ mod } 353) \text{ mod } 353$$

$$= 3 * 318 \text{ mod } 353 = 954 \text{ mod } 353$$

$$= 248$$

Now Common Secret key of A

$$K_{AB} = y_B^{xA} \text{ mod } 353$$

$$\begin{aligned}
&= 248^{97} \bmod 353 \\
&= 248 * (248^2 \bmod 353)^{48} \bmod 353 \\
&= 248 * (82)^{48} \bmod 353 \\
&= 248 * (82^2 \bmod 353)^{24} \bmod 353 \\
&= 248 * (17)^{24} \bmod 353 \\
&= 248 * (17^2 \bmod 353)^{12} \bmod 353 \\
&= 248 * 289^{12} \bmod 353 \\
&= 248 * (289^2 \bmod 353)^6 \bmod 353 \\
&= 248 * (213)^6 \bmod 353 \\
&= 248 * (213^2 \bmod 353)^3 \bmod 353 \\
&= 248 * (185)^3 \bmod 353 \\
&= 248 * (185 * (185^2 \bmod 353) \bmod 353) \bmod 353 \\
&= 248 * (185 * 337 \bmod 353) \bmod 353 \\
&= 248 * 217 \bmod 353 = 53816 \bmod 353 \\
&= 160
\end{aligned}$$

Now Common Secret key of B

$$\begin{aligned}
K_{AB} &= y_A^{x_B} \bmod 353 \\
&= 40^{233} \bmod 353 \\
&= 40 * 40^{232} \bmod 353 \\
&= 40 * (40^2 \bmod 353)^{116} \bmod 353 \\
&= 40 * (188)^{116} \bmod 353 \\
&= 40 * (188^2 \bmod 353)^{58} \bmod 353 \\
&= 40 * 44^{58} \bmod 353 \\
&= 40 * (44^2 \bmod 353)^{29} \bmod 353 \\
&= 40 * (171)^{29} \bmod 353 \\
&= 40 * (171 * 171^{28} \bmod 353) \bmod 353
\end{aligned}$$

$$\begin{aligned}
&=40 * (171 * (171^2 \text{ mod } 353)^{14} \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * 295^{14} \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [295^2 \text{ mod } 353]^7 \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187^7] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * 187^6 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * \{187^2 \text{ mod } 353\}^3 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * 22^3 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * \{22 * (22^2 \text{ mod } 353) \text{ mod } 353\} \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * \{22 * 131 \text{ mod } 353\} \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * [187 * 58 \text{ mod } 353] \text{ mod } 353) \text{ mod } 353 \\
&=40 * (171 * 256 \text{ mod } 353) \text{ mod } 353 \\
&=40 * 4 \text{ mod } 353 \\
&=160 \text{ mod } 353 \\
&=160
\end{aligned}$$