PAGE NO.
DATE / /

Example: N = 221
e = 5
calculate d = ?
also encrypt p = 7.

Solution: $221 = 13 \times 17$.

$p = 13$
$q = 17$

$\phi(221) = \phi(13 \times 17)$
$= 12 \times 16 = 192$.

$\phi(192) = \phi(2^6 \times 3)$
$= (2^6 - 2^5) \times 2$
$= 64$

$d = e^{-1} \bmod \phi(n)$
$= 5^{-1} \bmod 192$
$= 5^{\phi(192)-1} \bmod 192$.
$= 5^{63} \bmod 192$
$= 5^{32} \times 5^{16} \times 5^8 \times 5^4 \times 5^2 \times 5^1 \bmod 192$.
$= 1 \times 1 \times 97 \times 49 \times 25 \times 5^1 \bmod 192$
$= 77$

Encryption.

$C = p^e \bmod n$
$= 7^5 \bmod 221$
$= 7^{4+1} \times 7^2 \times 7 \bmod 221$.
$= 11$

Example: $p = 19$

$q = 23$

$e = 3$

find n, $\phi(n)$ and d?

Solution: $n = p \times q$

$= 19 \times 23 = 437.$

$\phi(437) = \phi(19 \times 23)$

$= 18 \times 22 = 396.$

$d = e^{-1} \bmod \phi(n)$

$= 3^{-1} \bmod 396.$

$= 3^{\phi(396)-1} \bmod 396.$

$= 3^{120-1} \bmod 396$

$= 3^{119} \bmod 396$

$= 3^{64} \times 3^{32} \times 3^{16} \times 3^{4} \times 3^{2} \times 3 \bmod 396.$

$= 81 \times 9 \times 333 \times 81 \times 9 \times 3 \bmod 396$

$= 279$

$\phi(396)$

$= \phi(2^2 \times 3^2 \times 11)$

$= (2^2 - 2) \times (3^2 - 3) \times 10$

$= 120.$