

Practical -5

Implement RSA algorithm.

Example of RSA Algorithm

I. Choose $p = 3$ and $q = 11$

II. Compute $n = p * q = 3 * 11 = 33$

III. Compute $\phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$

IV. Choose e such that $1 < e < \phi(n)$ and e and n are coprime. Let $e = 7$

V. Compute a value for d such that $(d * e) \% \phi(n) = 1$. One solution is $d = 3 [(3 * 7) \% 20 = 1]$

VI. Public key is $(e, n) \Rightarrow (7, 33)$

VII. Private key is $(d, n) \Rightarrow (3, 33)$

VIII. The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$

IX. The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$