RSA暗号

例

公開鍵：$n = 55, e = 7$

秘密鍵：$p = 5, q = 11,$

$\Phi(n) = (p-1)(q-1) = 40,$

$d = 23(7 \times 23 \; mod \; 40 = 1)$

平文：$M = 3$

暗号化 ： $C \equiv M^e \; mod \; n \quad 3^7 \equiv 42 \; mod \; 55$

復号化 ： $M \equiv C^d \; mod \; n \quad 42^{23} \equiv 3 \; mod \; 55$