RSA 暗号の暗号化と復号の計算の例

例として暗号化鍵は $(e,n)=(3,55)$ 復号鍵 $(d,n)=(27,55)$ の場合の暗号化と復号の手順を示す．$n=55$ なので，使用できる数値は 0 から 54 である．0 以上 55 未満の整数 M を暗号化する関数は

$$C \equiv M^e \pmod{55}$$

である．

例として，$M=7$ を暗号化する．暗号化の計算は

$$C \equiv M^e \pmod{n} \equiv 7^3 \pmod{55}$$

である．55 を法とした計算であることに注意して，$7^3=343\equiv 13 \pmod{55}$ として暗号文 $C=13$ を得る．

つぎに復号鍵 27 で暗号文 $C=13$ がもとの平文 $M=7$ に戻ることを確認する．復号化の計算は

$$C^d \pmod{n} \equiv 13^{27} \pmod{55}$$

ここで，大きい冪乗の値は電卓では正確な値が計算できないことに注意する．法を n とする計算なのでこのような場合は随時 n で割った余りで値を置き換え，値を小さく保ちながら計算してゆくことで手作業でも計算できる．具体的には，以下すべて法を $n=55$ とする計算として

$13^2 \equiv 4$

$13^4 \equiv (13^2)^2 \equiv 16$

$13^8 \equiv (13^4)^2 \equiv 256 \equiv 36$

$13^{16} \equiv (13^8)^2 \equiv 1296 \equiv 31$

などを順に求めておき，$13^{27} \equiv 13^{16}\cdot 13^8\cdot 13^2\cdot 13^1$ で求められる．ここでも部分的に積を求めてゆく．$13^{16}\cdot 13^8 \equiv 1116 \equiv 16$, $(13^{16}\cdot 13^8)\cdot 13^2 \equiv 16\cdot 4 \equiv 64 \equiv 9$, $((13^{16}\cdot 13^8)\cdot 13^2)\cdot 13^1 \equiv 9\cdot 13 \equiv 117 \equiv 7$, として元の平文 $M=7$ が得られることを確認できる．