RSA 暗号化について

1. 暗号の基本となるのはオイラーの定理と呼ばれるもの。特別の場合にフェルマーの小定理とも呼ばれる。encrypt の e、decrypt の d にたいして $ed \equiv 1(\mathrm{mod}\phi(\mathrm{n}))$ となるようになっている。$\phi(n) = (p-1)(q-1)$ である。また $n = pq$ である。これらの数に対して、不思議なことに $m^{\phi(n)} \equiv 1(\mathrm{modn})$ となるらしい。

   このため message の m を公開鍵 e で encrypt された crypt message の $c \equiv m^e(\mathrm{modn})$ は $c^d \equiv m^{ed} \equiv m(\mathrm{modn})$ で元に戻ってしまう。m^{ed} の中にいくつも $m^{\phi(n)}$ があってもそのあまりはいつも 1 であるからである。かけ算は余りのかけ算に同じとなる性質がある。