Public Key Cryptography

The RSA cryptosystem is a public key cryptosystem based on modular exponentiation, where the keys are pairs (e, n) consisting of an exponent e and a modulus n that is the product of two large primes; that is,

$$n = pq$$

where p and q are large primes, so that

$$(e, \phi(n)) = 1$$

To encrypt a message, we first translate the letters into their numerical equivalents and then form blocks of the largest possible size (with an even number of digits). To encrypt a plaintext block P, we form a ciphertext block C by

$$C \equiv P^e \pmod{n}, \quad 0 \leq C < n$$

Let

$$d \text{ be an inverse of } e \text{ modulo } \phi(n)$$

Note that d exists by Theorem 1 from Section 4.2, because $(e, \phi(n)) = 1$. To decrypt the ciphertext block C, we find

$$D(C) \equiv C^d \pmod{n}, \quad 0 \leq D(C) < n$$

By Theorem 3 from Section 1.5 (Division Algorithm), C and $D(C)$ are unique.

We now show that

$$D(C) \equiv P \pmod{n} \tag{1}$$

We have

$$D(C) \equiv C^d \equiv (P^e)^d = P^{ed} = P^{k\phi(n)+1} \equiv P^{\phi(n)k}P \pmod{n} \tag{2}$$

where

$$ed = k\phi(n) + 1$$

for some integer k, because $ed \equiv 1 \pmod{\phi(n)}$. We distinguish two cases:

Case A: Suppose $(P, n) = 1$. By Euler's theorem we have

$$P^{\phi(n)} \equiv 1 \pmod{n}$$

Consequently,

$$P^{\phi(n)k}P = (P^{\phi(n)})^k P \equiv P \pmod{n} \tag{3}$$

Clearly, (2) and (3) imply (1).

Case B: We now consider the rare case when $(P, n) > 1$. By (2) we have

$$D(C) \equiv P^{ed} \equiv P^{\phi(n)k}P \pmod{n}$$

therefore

$$D(C) \equiv P^{ed} \equiv P^{\phi(n)k}P \pmod{p} \tag{4}$$

We first suppose that $P \not\equiv 0 \pmod{p}$. Then

$$P^{\phi(n)k}P = P^{(p-1)(q-1)k}P = (P^{(p-1)})^{(q-1)k}P \equiv P \pmod{p}$$

since $P^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. We now suppose that $P \equiv 0 \pmod{p}$. Then by (4), we have

$$D(C) \equiv P^{ed} \equiv 0 \pmod{p}$$

So, $P \equiv 0 \pmod{p}$ and $D(C) \equiv 0 \pmod{p}$, therefore $D(C) \equiv P \pmod{p}$ in this case as well. Similar reasoning holds for the prime q, so that $D(C) \equiv P \pmod{q}$. We finally note that the system of congruences

$$\begin{cases} D(C) \equiv P \pmod{p} \\ D(C) \equiv P \pmod{q} \end{cases} \tag{5}$$

implies

$$D(C) \equiv P \pmod{n}$$

since any $D(C)$ of the form $nm + P$ satisfies (5) and, on the other hand, (5) has a *unique* solution $D(C)$ modulo $n = pq$ by the Chinese remainder theorem.

So, (1) holds for all P, including those P for which $(P, n) > 1$.

REMARK 1: Note that our reasoning in Case B also applies in Case A, although it is more complicated.

REMARK 2: Because $0 \leq D(C) < n$ and a block of ciphertext P is less than n, (1) implies

$$D(C) = P$$