THEOREM (NIB) 8 and the Proof that RSA works

THEOREM (NIB) 8

THEOREM (NIB) 8: Suppose p and q are two distinct primes and N is an integer, $N > 1$.
Then, If $p | N$ and $q | N$, then $pq | N$.

Proof: Suppose $p | N$ and $q | N$.
Then, there exists an integer k such that $N = pk$.
Since $q | N$, $q | pk$ by substitution.
Since q is a prime number and $q | pk$,
$q | p$ or $q | k$ by THEOREM (NIB) 2.
Since q and p are distinct primes, $q \nmid p$.
$\therefore$ $q | k$, by elimination.
$\therefore$ $k = q\ell$, for some integer ℓ.
$\therefore N = pk = p(q\ell)$
$\therefore N = (pq)\ell$.
$\therefore pq | N$.
QED.

PROOF THAT RSA ENCRYPTION / DECRYPTION WORKS
(Assuming that $M < pq$)

<u>Proof:</u> Let two distinct prime numbers p and q be given. Let $N = pq$ and

let e be a positive integer such that
$$\gcd(e, (p-1)(q-1)) = 1.$$
[N and e are the ENCRYPTION keys.]

Let d be a positive integer which is a (mod $(p-1)(q-1)$) inverse of e, that is,
$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$ Note that $ed \geq 1$.

[N and d are the Decryption keys.]

[We will use the notations "$a \equiv b \pmod{n}$" and "$a \equiv_{(\mathrm{mod}\, n)} b$" interchangeably.]

Let M be an integer such that $0 \leq M < pq$.

Let $C = (M^e \bmod pq)$. [C is the ciphertext of the plaintext M]

Let $M_1 = (C^d \bmod pq)$. [M_1 is the result of RSA Decryption of the Ciphertext C.]

[We need to show that $M_1 = M$.]

[Note that, by using large primes for p and q, it is reasonable to require that $0 \leq M < pq$.]

[Before beginning the proof argument, we present an outline of the argument for clarity.

We need to prove that $m_1 = m$.

We first prove that $m_1 = (m^{ed} \bmod pq)$.

We next prove that

$m^{ed} \equiv_{(\text{mod } p)} m$ and that $m^{ed} \equiv_{(\text{mod } q)} m$.

We will apply Theorem (NIB) 8 to prove that

$m^{ed} \equiv_{(\text{mod } pq)} m$.

Recall that

$0 \leq m < pq$. Then, by Thm (NIB) 6,

$(m^{ed} \bmod pq) = m$.

Thus, $m_1 = m$, by transitivity.]

[Part 1: Proving that $m_1 = (m^{ed} \bmod pq)$]

Recall $m_1 = (c^d \bmod pq)$ and $c = (m^e \bmod pq)$.

$m^e \equiv_{(\text{mod} pq)} (m^e \bmod pq)$, by Theorem (NIB) 4.

$\therefore (m^e)^d \equiv_{(\text{mod} pq)} (m^e \bmod pq)^d$, by Thm 8.4.3.

$\therefore m^{ed} \equiv_{(\text{mod} pq)} c^d$, by substitution.

$\therefore c^d \equiv_{(\text{mod} pq)} m^{ed}$, by symmetry of "$\equiv_{(\text{mod} pq)}$".

$\therefore (c^d \bmod pq) = (m^{ed} \bmod pq)$, by Thm 8.4.1.

[We just showed that $(c^d \bmod pq) = (m^{ed} \bmod pq)$.]

$\therefore$ Since $m_1 = (c^d \bmod pq)$, $\boxed{m_1 = (m^{ed} \bmod pq), \text{ by subst.}}$

[Part 2: Proving that $(m^{ed} \bmod pq) = m$]

Recall that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

$\therefore$ $(p-1)(q-1) \mid (ed-1)$, by def'n of congruence mod $(p-1)(q-1)$.

$\therefore$ $ed - 1 = (p-1)(q-1)k$ for some integer k.

$\therefore$ $ed = 1 + (p-1)(q-1)k$.

$\therefore$ $m^{ed} = m^{(1+(p-1)(q-1)k)}$.

$\therefore$ $m^{ed} = m \cdot m^{(p-1)(q-1)k}$.

$$\boxed{\therefore m^{ed} = m \cdot [m^{(p-1)}]^{(q-1)k} \text{ and } m^{ed} = m[m^{(q-1)}]^{(p-1)k}.}$$

<u>Internal Lemma</u>: For all integers $n > 1$,
if $n \mid m$, then $m^{ed} \equiv_{(\text{mod } n)} m$.

<u>Proof of the Internal Lemma</u>:

Let n be any integer, $n > 1$, such that $n \mid m$.

$\therefore n \mid (m - 0)$. $\therefore m \equiv_{(\text{mod } n)} 0$, by def'n of "$\equiv_{(\text{mod } n)}$".

$\therefore m^{ed} \equiv_{(\text{mod } n)} 0^{ed}$, by Theorem 8.4.3.

$\therefore m^{ed} \equiv_{(\text{mod } n)} 0$ and $0 \equiv_{(\text{mod } n)} m$, by symmetry;

thus $m^{ed} \equiv_{(\text{mod } n)} m$, by Transitivity. QED for the Internal Lemma.

[PART 2A: Proving that $m^{ed} \equiv_{(\text{mod } p)} m$.]

Note that, in the case that $p \mid m$, $m^{ed} \equiv_{(\text{mod } p)} m$, by the Internal lemma.

We assume, then, that $p \nmid m$.

$\therefore$ By Fermat's Little Theorem (Thm 8.4.10),

$$m^{(p-1)} \equiv_{(\text{mod } p)} 1.$$

Recall that $m^{ed} = m\left[m^{(p-1)}\right]^{(q-1)k}$.

By Theorem 8.4.3, $m \cdot \left[m^{(p-1)}\right]^{(q-1)k} \equiv_{(\text{mod } p)} m \cdot 1^{(q-1)k} = m$

$\therefore m^{ed} \equiv_{(\text{mod } p)} m$ in the case that $p \nmid m$, by transitivity.

$\boxed{\therefore m^{ed} \equiv_{(\text{mod } p)} m, \text{ in general.}}$

[Part 2B: Proving that $m^{ed} \equiv_{(\text{mod } q)} m$.]

Because $m^{ed} = m \cdot \left[m^{(p-1)}\right]^{(q-1)k}$ and $m^{ed} = m \cdot \left[m^{(q-1)}\right]^{(p-1)k}$, the argument in Part 2A provides a proof that $m^{ed} \equiv_{(\text{mod } q)} m$, when the roles of p and q are reversed. $\boxed{\therefore m^{ed} \equiv_{(\text{mod } q)} m.}$

$\therefore p \mid (m^{ed} - m)$ and $q \mid (m^{ed} - m)$.

By Theorem (N1B) 8, $pq \mid (m^{ed} - m)$.

$\boxed{\therefore m^{ed} \equiv_{(\text{mod } pq)} m.}$

$\therefore$ Since $m^{ed} \equiv_{(\text{mod } pq)} m$ and $0 \leq m < pq$,

$\boxed{(m^{ed} \text{ mod } pq) = m \text{, by Theorem (NIB) 6.}}$

Since $m_1 = (m^{ed} \text{ mod } pq)$ and $(m^{ed} \text{ mod } pq) = m$,

$m_1 = m$, by Transitivity.

$\therefore$ RSA ENCRYPTION / DECRYPTION WORKS.

QED.