Facts Related to Paillier Encryption

Fact 1. *For any a, b relatively prime, $\phi(ab) = \phi(a)\phi(b)$.*

Proof. Let A be the set of positive integers less than and relatively prime to a, let B be the set of positive integers less than and relatively prime to b, and let C be the set of positive integers less than and relatively prime to ab. We show that the Chinese Remainder Theorem establishes a bijection between the sets $A \times B$ and C; hence C must have cardinality $|A||B| = \phi(a)\phi(b)$.

Consider the mapping $f : C \to A \times B$ which takes $x_C \in C$ to pairs $(x_A, x_B) = (x_C \pmod a, x_C \pmod b)$. Note that $x_C = \alpha a + x_A = \beta b + x_B$ for some integers α, β. We first prove the fact that $(x_C, ab) = 1 \iff (x_A, a) = 1$ and $(x_B, b) = 1$. If some $k | x_A$ and a, then $k | x_C = \alpha a + x_A$ and $k | a$. To see the other direction, note that if $(x_C, ab) = k$ then either $(x_C, a) = k$ or $(x_C, b) = k$. WLOG, assume the former: we have that $(x_C, a) = (x_A, a) = 1$ (we proved this for Euclid's algorithm). Now we have that f is well-defined, and the Chinese Remainder Theorem gives that it is a bijection since any pair $(x_A, x_B) \in A \times B$ corresponds to exactly one solution $x_C \in C$. ■

Fact 2. *For any $n = pq$ where p and q are primes, $\phi(n^2) = n \cdot \phi(n) = n(p-1)(q-1)$.*

Proof. By the fact above we have that $\phi(n^2) = \phi(p^2q^2) = \phi(p^2)\phi(q^2)$. Since p is prime, all p^2 residues except the multiples of p are relatively prime to p^2. Thus $\phi(p^2) = p^2 - p$ and similarly $\phi(q^2) = q^2 - q$. This gives that

$$\phi(n^2) = (p^2 - p)(q^2 - q) = p(p-1)q(q-1) = n(p-1)(q-1) = n \cdot \phi(n).$$

■

Fact 3. *Let $n = pq$ for primes p and q and let $k \equiv v \pmod n$. Then $(1+n)^v \equiv (1+n)^k \pmod{n^2}$.*

Proof. By assumption $v = \alpha n + k$ for some integer α. Then

$$(1+n)^v = (1+n)^{\alpha n + k} = (1+n)^{\alpha n}(1+n)^k,$$

and we only need to show that $(1+n)^{\alpha n} \equiv 1 \pmod{n^2}$. Applying the binomial theorem gives that $(1+n)^{\alpha n} = 1^{\alpha n} + \binom{n}{1} 1^{\alpha n - 1} n + \ldots$ and it is easy to see that n^2 divides all the terms except the first, so $(1+n)^{\alpha n} \equiv 1 \pmod{n^2}$. ■

Fact 4. *Let $n = pq$ for primes p and q, let $r_1, r_2 \in \mathbb{Z}_n^*$, and let $k = r_1 r_2 \pmod n$. Then $(r_1 r_2)^n \equiv k^n \pmod{n^2}$.*

Proof. By assumption, $r_1 r_2 = \alpha n + k$ for some integer α. Thus

$$(r_1 r_2)^n = (k + \alpha n)^n = \sum_{i=0}^{n} \binom{n}{i} k^{n-i} \cdot (\alpha n)^i.$$

Now n^2 divides each term for $i > 0$ so $(k + \alpha n)^n \equiv k^n \equiv \pmod{n^2}$. ■