The RSA cipher

- ## The keys for user A

A chooses two large prime numbers p and q and calculates $n = pq$. A then chooses $d \in \mathbb{Z}^*_{\phi(n)}$ and calculates the multiplicative inverse e of d, that is, $ed \equiv 1 \pmod{\phi(n)}$.

A keeps the keys p, q and d secret, but makes the keys n, e public — you will need the public keys when you need to send a message to A.

- ## Encryption

If you want to send the message $x \in \mathbb{Z}_n$ to A, you encrypt x by the rule

$$e(x) \equiv x^e \pmod{n}$$

Decryption

A receives the cipher y and then decrypts by the rule

$$d(y) \equiv y^d \pmod{n}$$

We need to prove that $d(y) = x$, that is, that $d(e(x)) \equiv x \pmod{n}$.

Proof: $d(e(x)) \equiv d(x^e) \equiv (x^e)^d \equiv x^{ed} \pmod{n}$.

So, we need to prove that $x^{ed} \equiv x \pmod{n}$.

We know that $ed \equiv 1 \pmod{\phi(n)}$, and therefore $ed = i\phi(n) + 1$ for some integer i, and therefore $x^{ed} \equiv x^{i\phi(n)+1} \pmod{n}$.

So, we need to prove that $x^{i\phi(n)+1} \equiv x \pmod{n}$.

If $x^{i\phi(n)+1} \equiv x \pmod{p}$ and $x^{i\phi(n)+1} \equiv x \pmod{q}$, then, by Lemma 6, $x^{i\phi(n)+1} \equiv x \pmod{n}$.

We prove that $x^{i\phi(n)+1} \equiv x \pmod{p}$:

If x is divisible by p, then

$x \equiv 0 \pmod{p}$, and therefore

$x^{i\phi(n)+1} \equiv x \pmod{p}$ in this case.

If x is not divisible by p, then by Fermat's Little Theorem

$$x^{p-1} \equiv 1 \pmod{p}$$

$$\therefore \left(x^{p-1}\right)^{q-1} \equiv 1 \pmod{p}$$

$$\therefore x^{(p-1)(q-1)} \equiv 1 \pmod{p}$$

$$\therefore x^{\phi(n)} \equiv 1 \pmod{p}$$

$$\therefore x^{i\phi(n)+1} \equiv x \pmod{p}$$ in this case too.

Similarly, $x^{i\phi(n)+1} \equiv x \pmod{q}$, and

therefore $x^{i\phi(n)+1} \equiv x \pmod{n}$ ∎