# 6 RSA Encryption

The idea behind all forms of ”trap door encryption” is to have some function that’s easy to do forward, but nearly impossible to do in reverse, unless you know some secret. Crypto people traditionally talk about Alice and Bob when describing algorithms.

If Alice wants anybody to be able to securely communicate with her, she creates two ”keys”; a ”public key” and a ”private key”. She ”publishes” (makes available to everyone) the public key, but keeps the private key secret. Anybody can take the public key and use it to encrypt a message. This turns ”text” into ”cyphertext”. So if Bob wants to send Alice a message, he can encrypt it with her public key, and then publish the cyphertext. Alice can then take that cyphertext and ”decrypt” it using her private key.

It’s easy for anyone to encrypt a message (forward operation), but it’s very difficult to recover the original text without the private key (reverse operation). ”Difficult” for a cryptographer often involves phrases like ”all of the world’s computing power for many ages of the universe”.

## 6.1 the algorithm

Say you’ve got three large numbers, $M$, $k$, and $\ell$, such that $[k \cdot \ell]_{\phi(M)} = 1$. That is; $k \cdot \ell = j\phi(M) + 1$, for some $j$.

Encrypting with the public key, $k$, is simply raising the text $T$ to the power $k$ modulo $M$. So the cyphertext, $C$, is $C = [T^k]_M$. Decrypting means raising the cyphertext, $C$, to the power $\ell$, which recovers the original $T$.

**Q 5.1.1**: Show that when $gcd(T, M) = 1$, $[C^\ell]_M = T$.

**Q 5.1.2**: Using the Chinese remainder theorem decomposition, show that even when $gcd(T, M) \neq 1$, $[C^\ell]_M = [T^{j\phi(M)+1}]_M = T$. Keep in mind that $M = PQ$, where $P$ and $Q$ are prime.

Hint: When $gcd(T, M) \neq 1$ the decomposition looks like $([?]_P, [?]_Q)$

So, how do you generate $M$, $k$, and $\ell$? Start with two large random primes, $P$ and $Q$. $M$ is just the product, $M = PQ$. Then generate a completely random $k < M$, such that $gcd(k, \phi(M)) = 1$. By definition, $[\ell]_{\phi(M)} = [k^{-1}]_{\phi(M)}$. The fact that the inverse needs to exist is why you need $gcd(k, \phi(M)) = 1$.

**Q 5.1.3**: -If you’re given a very large number, $P$ or $Q$, how do you quickly check that it is (most likely) prime?

-How do you quickly check that whether or not $gcd(k, \phi(M)) = 1$?

-How do you quickly find $\ell$?

**Q 5.1.4**: $M = 35$, $k = 5$, $\ell = 5$, and $T = 7$.

-Check that these numbers meet the requirements for being a public key.

-Find the cyphertext, $C$.

-Verify that $[C^{\ell}]_M = T$.

**Q 5.1.5**: Paul Revere has given you a public key, $M = 77$, $k = 7$, and you've agreed that when the British arrive you'll encrypt and send a message. "2" if by sea or "3" if by land. Suddenly the evil British arrive... by sea.

-What cypertext will you send?

-Revere's public key is weak. "Break it" by finding the secret key, $\ell$.

**Q 5.1.6** -Pick two primes, $P$ and $Q$, between 2 and 100. Find $M = PQ$ and $\varphi(M)$.

-Pick a $k$ such that $gcd(k, \varphi(M)) = 1$. Find $\ell$ such that $k\ell = j\varphi(M) + 1$.

-Give $M$ and $k$ to someone else (they could be sitting right next to you). Ask them to encrypt a secret message, like "7", and give the cyphertext back to you.

-Use the secret key, $\ell$, to find the original secret message.