RSA Encryption

RSA is an algorithm for sending secret messages publicly that is based on the presumed difficulty of factoring large integers.

In the RSA system, each user sets up his or her own public and private keys. The public keys are "very" public — they are published in some location so that everyone who wants to can find them. The private keys need to be kept "very" private. If anyone (besides the one user who owns them) has access to them, then that person can read any secret messages sent to the rightful owner of the key.

Algorithm:

Pick primes: The first step is to pick two prime numbers p and q. In practice, these primes need to be very large — about 150 digits each.

- We'll take p=3 and q=11.

Calculate n and φ(n): Next, simply sets n = pq. Because we know the factorization of n, she can compute φ(n) = (p − 1)(q − 1). Notice that in practice, n will have about 300 digits. This means that computing φ(n) would be very difficult without knowing the factorization of n, and factoring n would also be very difficult.

- In our example, we have n=(3)(11)=33 and φ(n) = (2)(10) = 20.

Choose e — the encoding exponent: The next step is to pick a value of e less than n at random, making sure that e, φ(n) have no factors in common except 1. There is mathematical theory that can help you find an e.

- We will take e=3. Notice that the factors of 3 are 1 and 3 and the factors of 20 are 1, 2, 4, 5, 10, 20 so 3 and 20 do not have any factors in common.

Find d — the decoding exponent: Now, we need to find a value of d so that $de \equiv 1 \pmod{\varphi(n)}$. Once again there is mathematical theory that can help us find our d.

- In our example we want d so that 3d= 1 mod 20. Observe that d=7 works as 7x3=21=1 mod 20.

Publish the public keys: n = 33 and e = 3.

Private key: d=7

Keep secret the private key: d = 7. Incidentally, we should also destroy our records of p, q, and φ(n). These bits of information are no longer needed, and if anyone else finds them, they will be able to figure out her (private) decoding exponent d.

Encode: To encode the message "HI".

1. Remember from our simple coding (A=1, B=2,…) that H=8 and I=9.
2. To encode our letters we do the following:
   - H→ $8^e = 8^3 \bmod 33 = 17$
   - I → $9^e = 9^3 \bmod 33 = 3$
3. Send 17, 3

Decode: To decode an encoded message 17, 3.

1. $17^d = 17^7 = 8 \bmod 33$ → H
2. $3^d = 17^7 = 9 \bmod 33$ → I