

## RSA Cryposystem

RSA stands for Rivest, Shamir, Adleman. These are the three men who, in 1977, invented this method of encrypting messages. This method is now used extensively in computer systems around the world. It is based on the idea that **factoring large numbers is hard**. When we say large, we mean in the hundreds of digits long. The point of RSA is that anyone can *encrypt* a message, but only the person to whom the message was sent is able to *decode* the message. This is important for things like using a credit card on the Internet. Sellers like Amazon.com need to be able to tell your computer how to send them a secret message, without telling everyone else how to decode the message at the same time.

Here is an example of how RSA works. Alice would like to send a secret message to Bob. So Bob has to work through some numbers so he can tell Alice how she should do this. Bob picks two prime numbers. For this example, he picks two smallish primes, but in reality they would each be at least one hundred digits long. So he picks

$$P = 61 \quad Q = 53$$

He then multiplies them together to get

$$PQ = 3233$$

The whole idea is that this number is hard to factor. You'll see why this is important later.

Bob can now give Alice two numbers to use: 3233, and another number that has no factors in common with  $(P - 1)(Q - 1) = 3120$ , for instance,  $E = 17$ .

Alice wants to meet Bob at Abe's Diner, so to keep her message short she decides to send the message ABE. This could be turned into numbers in different ways, but we will use the standard "A = 1, B = 2, ..., Z = 26", so that ABE  $\rightarrow$  125. Now to make this number secret, she performs the following calculation:

$$\begin{aligned} M^E \text{ mod } PQ &\equiv 125^{17} \text{ mod } 3233 \\ &\equiv 1516 \text{ mod } 3233 \end{aligned}$$

She sends Bob the number 1516. Now Bob has to do something with this. He knows a theorem that says that there exists a number  $d$  such that  $(M^E)^d \equiv M^{Ed} \equiv M \text{ mod } PQ$ , and that you solve for  $d$  by solving  $Ed \equiv 1 \text{ mod } (P - 1)(Q - 1)$ . So he just has to find the number  $d$  such that  $17d \equiv 1 \text{ mod } (52)(60) \equiv 1 \text{ mod } 3120$ .

It turns out that this number is  $d = 2753$ . So all Bob has to do is solve

$$\begin{aligned} (M^E)^d \text{ mod } PQ &\equiv (1516)^{2753} \text{ mod } 3233 \\ &\equiv 125 \text{ mod } 3233 \end{aligned}$$

which he translates as ABE.

Without knowing  $(P - 1)(Q - 1)$ , Bob could not have found his number  $d$  which allowed him to decrypt the message. So the message is secure as long as  $PQ$  is hard to factor.