RSA Cryptosystems

A public-key cryptosystem works on the basis of making public two pieces of information, $n$ and $k$, such that the sender (A) and receiver (B) of information know something extra about the number $n$. In particular, $n$ is usually chosen to be equal to the product of two (massive and distinct) prime numbers, $p$ and $q$, known by A and B but NOT known to the public. In general, $p$ and $q$ are extremely difficult to find, and this is where the security of the system arises. Now,

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

We then choose $k$ such that $(k, \phi(n)) = 1$. Then B finds $j < n$ such that

$$kj \equiv 1 \mod \phi(n).$$

It is then the case that using the $n$, $k$, and $j$ defined here,

$$a^k \equiv r \mod n \iff r^j \equiv a \mod n. \quad (1)$$

Using the legend presented in class (also on web page), where “99” corresponds to a space, let’s say A wishes to encode the following message: “MATH IS FUN”

We will let $M$ denote the character representation of A’s message, that is,

$$M = 12001907990818052013.$$

So, A will pick two primes numbers, say $p = 127$ and $q = 8191$, and then $n = pq = 1040257$. Now $\phi(n) = (p-1)(q-1) = 1031940$, and A can pick $k = 10007$ because then $(10007, 1031940) = 1$. Now, A breaks up $M$ into blocks of code, that is $M = M_1M_2M_3M_4$ where

$$M_1 = 12001,$$
$$M_2 = 90799,$$
$$M_3 = 08180,$$
$$M_4 = 52013,$$

and A raises each of the $M_i$ to the $k$ and takes the result modulo $n$.

$$M_1^k \equiv 609084 \mod n$$
$$M_2^k \equiv 204679 \mod n$$
$$M_3^k \equiv 710714 \mod n$$
$$M_4^k \equiv 610958 \mod n$$
A then writes a new number \( r \), which is the concatenation of those numbers just found, where each is made to have the same length as \( n \) by adding zeros to the front, that is,

\[
r = 0609084|0204679|0710714|0610958,
\]

where the bars denote the four different blocks. This number is then sent to B as the encoded information.

B receives the number \( r \) and needs to undo the encoding to recover the message \( M \). To do this they will use (1) from above. The first step is to find \( j \) such that \( kj \equiv 1 \mod \phi(n) \), and they obtain that \( j = 165923 \). Now B breaks up \( r = r_1r_2r_3r_4 \) into blocks of length \( n \), and applies (1) to recover the blocks of \( M \).

\[
\begin{align*}
  r_1^j &\equiv 12001 \mod n \\
  r_2^j &\equiv 90799 \mod n \\
  r_3^j &\equiv 8180 \mod n \\
  r_4^j &\equiv 52013 \mod n
\end{align*}
\]

Once they know that the original blocks were size 5 in length, B can then recreate

\[
M = 12001|90799|08180|52013,
\]

which reads as “MATH IS FUN”.