A Tiny Example of the RSA Algorithm

Dr Holmes

April 30, 2013

Our public information is a number $N$ and a number $r$. These numbers are available to anyone; anyone can send a message $M$ to us by encrypting it as $M' = M^r \mod N$.

Our private information is that we know how to factor $N$ into primes $p$ and $q$. Moreover, we chose $r$ so that it would be relatively prime to $(p-1)(q-1) = \phi(N)$.

Further, we compute the decryption exponent $s$ to be $r^{-1} \mod N$. We decode messages $M'$ by computing $(M')^s \mod N$: this works because $(M')^s \mod N = (M^r)^s \mod N = M^{rs} \mod N = M^{rs \mod \phi(N)} \mod N$, which is $M \mod N = M$ (we assume that $0 < M < N$). Remember that $s$ is the multiplicative inverse of $r \mod (p-1)(q-1) = \phi(N)$, which is why the last steps work.

We do an example of the kinds of problems in the worksheet with ridiculously small primes.

Let $N = 55$. Let $r = 3$.

The problems:

1. Encrypt 14.
2. Find the decryption exponent.
3. Decrypt 12.

To encrypt 14 compute $14^3 \mod 55 = 49$. 49 is the encrypted message.

To find the decryption exponent, we need to know $p$ and $q$, which are not a very well keep secret (5 and 11). Notice that $r = 3$ is relatively prime to $(p-1)(q-1) = 4 \times 10 = 40$.

The decryption exponent $s$ will be the reciprocal of 3 in mod 40 arithmetic.
40 1 0
3 0 1
1 1 -13 13

The reciprocal is $-13 = 40 - 13 = 27$ in mod 40 arithmetic.
To decrypt the message 12, compute $12^{27 \mod 55} = 23$: the original message was 23.

To do further checks, try decrypting 49 (you should get 14) and encrypting 23 (you should get 12).