THE RSA SYSTEM OF ENCRYPTION

MATH 5020 - MIKE ZABROCKI

The **receiver** picks two very large prime numbers p and q and sets $n = pq$ and then chooses a number e which is relatively prime to $\phi(n)$ (the Euler-phi function of n). Both n and e are given to anyone who cares to send a message to the receiver, however p, q and $\phi(n)$ are kept secret from everyone else.

The **sender** takes the numbers e and n from the receiver and then converts the message into a number m (this can be done anyway they feel like, just as long as the sender and receiver agree on a convention) and then transmits to the receiver $r \equiv m^e \ (mod\ n)$.

The receiver can decrypt the message by computing $r^d \ (mod\ n)$ where $d \equiv e^{-1} \ (mod\ \phi(n))$ because by the Euler-Fermat theorem $r^d \equiv (m^e)^d \equiv m^{ed} \equiv m \ (mod\ n)$. Anyone who knows both e and $\phi(n)$ can do the same computation so this is why it is important that the sender keep $\phi(n)$ secret.

The **opponent** may break this code by factoring n into its prime factors pq because then the opponent knows $\phi(n) = \phi(pq) = (p-1)(q-1)$ and then can compute $d \equiv e^{-1} \ (mod\ \phi(n))$ and then the message $m \equiv r^d \ (mod\ n)$. If we choose p and q to be really, really big prime numbers (at least 100 digits each) then factoring n is a hard problem and the opponent will be unable to factor the number without an enormous amount of resources.

Use a computer to answer the following questions (a computer can factor these but pretend that the encryption is large enough that it is secure):

(1) You are the sender. You will be sending the word 'DATELINE = 0401200512091405' to the receiver who has chosen a modulus $n = 2905554057268138607$ and $e = 61223183$. Find the message to send.
(2) You are the receiver, let $n = 1813739439517193 = 29384712 \cdot 61723849$ and $e = 187247$ and $d = 251089477478663$. A sender sent you the message, 298772360895187. Determine what message is being sent to you.
(3) You are the opponent. You intercept the message 88323309815619362318 37859 and you know that it was sent with the public modulus $n = 343795168794861048808 97911$ and encrypting exponent $e = 2343490992813$. Determine the message.

Remark: on Maple you may compute $a^b \ (mod\ n)$ with the command `a&^b mod n;`. The value of $\phi(n)$ is `phi(n);` and to factor n there is a command `ifactor(n);`. To compute the inverse of a modulo n use `a&^(-1) mod n;`.