

The R.S.A system. For the following problems, the same notations will be kept. First, the sender takes two large primes p, q , and forms $n = p \cdot q$. He also picks an integer e such that e and $\phi(n)$ are coprime. The message to be sent is an integer P (less than n , and coprime with n). The encrypted message C is given by $C \equiv P^e \pmod{n}$. At this point, p, q are only known to the sender, but n, e, C are public. Now the recipient of the message has a key, that is not public: the key d is an integer such that $d \cdot e \equiv 1 \pmod{\phi(n)}$, or equivalently such that $e \cdot d = k \cdot \phi(n) + 1$, for some k . Now deciphering the encrypted message C is easy: the recipient of the message just needs to perform $C^d \equiv P^{e \cdot d} \equiv P^{k \cdot \phi(n) + 1} \equiv P \pmod{n}$, thanks to Fermat's theorem. For these problems, you need also to remember that factorizing a large number is really hard, but finding a G.C.D. is not...

Problem 1. Show that if the message P is not coprime with n , then just knowing $C = P^e$ and n , one can recover p, q . If both p, q have 100 digits, what is the probability of producing such a message P that is not coprime with n ?

Problem 2. Suppose that you have two groups of recipients. Both of them use the same number n , but use two different exponents e_1, e_2 such that $\text{G.C.D.}(e_1, e_2) = 1$. Assume that the same message P is sent to the two groups. Therefore you have two public crypted messages $C_1 \equiv P^{e_1}$ and $C_2 \equiv P^{e_2}$. Show that knowing these two encrypted messages one can recover the initial message P .

Problem 3. Here we suppose that we have three senders, using different integers n_1, n_2, n_3 , but using the same exponent $e_1 = e_2 = e_3 = 3$. Show that if these three senders encrypt the same message P (thus producing three public crypted messages $C_i \equiv P^3 \pmod{n_i}$), then one can recover the initial message P .

Problem 4. Assume you are a bit paranoid and you encrypt your message P using n, e_1 to produce $C = P^{e_1} \pmod{n}$, and then encrypt one more time, using n, e_2 (same n) to produce the final (public) crypted message $D = C^{e_2} \pmod{n}$. Show that in reality you will not gain much by doing this.

Problem 5. Read the proof of the quadratic reciprocity that I gave on the web page. Ask me (at least) one question about it in class next week.