

The R.S.A system.

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 ?

Answer. If the message P is not coprime with n , then it must be a multiple of one of the prime factors, say p . Since the message is smaller than n it can't be a multiple of n . Thus $\text{G.C.D.}(n, P^e) = p$, and therefore we can retrieve the factors of n . There are $\phi(n) = n \cdot (1 - \frac{1}{p}) \cdot (1 - \frac{1}{q})$ integers coprime with n and less than n so the probability of being coprime with n is $\frac{\phi(n)}{n} = (1 - \frac{1}{p}) \cdot (1 - \frac{1}{q}) \simeq 1 - \frac{2}{10^{100}}$, and the probability of not being coprime is really low (of order $\frac{2}{10^{100}}$).

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 .

Answer. Since $\text{G.C.D.}(e_1, e_2) = 1$ we know the existence of integers a, b such that $ae_1 + be_2 = 1$. We can assume $a > 0$ and $b < 0$, therefore $ae_1 = 1 - be_2$ (equality between positive integers). But now $C_1^a = P^{ae_1} = P.P^{e_2 \cdot (-b)} = P.C_2^{-b}$, so we can find P , because C_1, C_2 are known.

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 .

Answer.

- If one of the pairs (n_i, n_j) is not made of coprime integers, then we can easily compute the G.C.D. of the pair which would be one factor in the factorisation of n_i (and therefore we would be done);
- We assume now that all the pairs are coprime: we can apply the chinese remainder theorem which says that the following map is an isomorphism

$$\mathbb{Z}/n_1n_2n_3 \rightarrow \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \mathbb{Z}/n_3$$

and therefore one can find an integer C such that $C \mapsto (C_1, C_2, C_3) = (P^3, P^3, P^3)$, therefore $C \equiv P^3 \pmod{n_1n_2n_3}$. But since P^3 is an integer less than $n_1n_2n_3$, we can simply compute its cubic root (as a real number!), and get the answer.

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

Answer. If you encrypt twice, your crypted message becomes $(P^{e_1})^{e_2} \bmod n$. So it is the same as using $(n, e_1 e_2)$ for the encryption. But now the problem of finding an inverse of $e_1 e_2 \bmod \phi(n)$ has exactly the same difficulty as the problem of finding an inverse for e_1, e_2 .

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.*

"Is it on the test?"