After a couple of hours of detailed study I've come to an answer.

As we all know the RSA algorithm works as follows:

17

- Choose two prime numbers p and q,
- Compute the modulus in which the arithmetic will be done: $N = pq$,
- Pick a public encryption key $e \in Z_n$,
- Compute the private decryption key as $d \mid ed = 1 \; mod \; \phi(N)$,
- Encryption of message m: $c = m^e \; mod N$,
- Decryption of crypto message c: $m = c^d \; mod N$.

While these statements and equations can stand true for some fixed values of p, q, m, e, d in order to define the RSA as a general cryptographic algorithm we must prove their generality for any message m we wish to encrypt.

This is therefore the reason why the proof of the correctness of the RSA algorithm is needed.

Getting to the proof we can formalise it as follows:

Hypothesis:

- $GCD(p, q) = 1$
- $N = pq$
- $ed = 1 \; mod \; \phi(N)$

Thesis:

- $(m^e)^d = m \; mod N \; \forall m \in Z_n$

> NOTE:The important part is ^^^^^^^^^ the for all part...

Proof:

Being $m \in Z_n$ there are only two possible cases to analyse:

> 1) $GCD(m, N) = 1$

In this case Euler's Theorem stands true, assessing that

$$m^{\phi(N)} = 1 (mod N).$$

As for the Thesis to prove, because of Hypothesis number 3, we can write:

$$(m^e)^d = m^{ed} = m^{1+k\phi(N)},$$

furthermore

$$m^{1+k\phi(N)} = m * m^{k\phi(N)} = m * (m^{\phi(N)})^k,$$

and for Euler's Theorem

$$m * (m^{\phi(N)})^k = m (mod N).$$

Proving that the thesis stands in this case.

> 2) $GCD(m, N) \neq 1$

In this case Euler's Theorem does not stand true any more.

For a result of the Chinese Remainder Theorem (check this SO question - Chinese Remainder Theorem and RSA - or just wiki it) it is true that if $GCD(p, q) = 1$ then:

$$x = y (mod p) \land x = y (mod q) \Rightarrow x = y (mod pq)$$

So by proving the following two statements we would have finished:

- $(m^e)^d = m \; mod p$,
- $(m^e)^d = m \; mod q$.

Because $GCD(m, N) \neq 1$ one between $GCD(m, N) = p$, and $GCD(m, N) = q$ must stand true. I will demonstrate that both the above statements stand true in the case $GCD(m, N) = p$, being it absolutely identical (by switching letters) to prove it for $GCD(m, N) = q$ as well.

So let it be $GCD(m, N) = p$, this implies that $m = kp$ for some $k > 0$ which means that $m mod p = 0$. By concerning the first statement we also have

$$(m^e)^d = ((kp)^e)^d$$

(me)d=((kp)e)d

which therefore results to be a multiple of p, and so it is equal to zero.

So the first statement becomes $0 = 0$ and is proven to be satisfied.

Concerning the second statement we have that Euler's Theorem results to be proved in Z_q since $GCD(m, q) = 1$, so:

$$m^{\phi(q)} = 1(mod q).$$

mϕ(q)=1(modq).

This implies that we can write:

$$\begin{aligned}(m^e)^d &= m^{ed} \\ &= m^{ed-1} m \\ &= m^{h(p-1)(q-1)} m \\ &= (m^{q-1})^{h(p-1)} m \\ &= 1^{h(p-1)} m = m mod q.\end{aligned}$$

(me)d=med=med−1m=mh(p−1)(q−1)m=(mq−1)h(p−1)m=1h(p−1)m=mmodq.

which definitively proves the second statement and theorem.

share improve this answer

edited Apr 13 at 12:48
Community ♦
1

answered Jun 13 '12 at 20:49
Matteo
600 2 7 21

2 you wrote "e ∊ Zn"; but e should be chosen with this criteria gcd(ϕ(N),e)=1 ; in other words e should be coprime with ϕ(N). See here crypto.stackexchange.com/questions/12255/… – Jako Jun 12 '16 at 16:38

add a comment