pqpq

defkit

November 14, 2022

Abstract

GCDGCDGCD, Rabin Cryptosystem. DTRUSH pqpq writeup

1 Factoring

We have public modulus for RSA $n = pqr$, where p,q,r are primes. And public exponent $e = 65537 * 2$, so we understand, that we will have problems in future after factorization, because of
GCD(e,phi) != 1.
And we have a hints
$p^e - q^e \mod n$ and $(p-q)^e \mod n$
The second hint we can compute as binomial. If we substract second and first hints, we receive something, that is dividing by q. So we compute gcd to find q. Then we substract first and second to find p. After this we find r.
We find the Eulers totient, and inverse of $d = 65537 \mod phi$
So $c^d \mod n = m^2 \mod n$. So we need to retrive m from this equation. This equation is something like Rabin cryptosystem.

2 Rabin cryptosystem with 3 primes

It is the same thing as Rabin cryptosystem. We just find 3 quadric residues and solve crt.
$x1 : x1^2 = m^2 \mod p$
$x2 : x2^2 = m^2 \mod q$ and so on.
But for every x, -x is a root too. So we have 8 equations, 2 of them are correct.