Problem Proposals

Eric Du

April 5, 2023

Alternate Berlekamp-Welch

Recall that Berlekamp-Welch requires that we write the Error locator polynomial $E(x)$ as:

$$E(x) = (x - e_1)(x - e_2) \cdots (x - e_k)$$

What if we redefine $E(x)$ to instead return 0 at a *correct point* instead? In this scheme, the degree of $E(x)$ would be $n - k - 1$, for a length n message with k corruptions. Note also that in this formulation of Berlekamp-Welch, we cannot use the normal equation $P(i)E(i) = r_i E(i)$, since $E(i) \neq 0$ at an error. How many packets would be required to successfully recover the message in this scheme?

RSA Correctness

Firstly, this does not hold for all m. For instance, take $m = 4$ and $e = 3$, a quick computation shows that $d = 3$ as well, so we want to show that

$$x^9 \equiv x \pmod 4$$

But this isn't even true for all x: take $x = 2$, which gives $x^9 \equiv 0 \pmod 4$, which violates the expression.

But okay, let's prove something slightly weaker: let $m = p - 1$ for some prime p. We prove that under this scheme, $x^{ed} \equiv x \pmod m$ does hold.

Firstly, $ed \equiv 1 \pmod m$. From here onwards, it will be useful to write $p - 1$ instead of m, so I will do that. From $ed \equiv 1 \pmod{p-1}$, we can then rewrite this as $ed = k(p - 1) + 1$. Therefore, we are asked to prove:

$$x^{k(p-1)+1} \equiv x \pmod m$$