NSUCRYPTO23 Problems

October 23, 2023

Problem 2.

From the idea of Euler (the polynomial $n^2 + n + 41$, which generate primes from 0 to 39), we can choose polynomial to generate such prime numbers. For example, according to https://mathworld.wolfram.com/Prime-GeneratingPolynomial.html, we can choose the sequence

$$a_n = \frac{1}{4}(n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316)$$

The sequence a_n generate distinct prime numbers for $n = 0, 1, 2, \ldots, 56$, hence its sequence primality parameter is equal to 57.
If the primes are not necessary distince, then we can choose

$$a_n = (n-2)! \cdot (n-2) \pmod{n} + 2$$

By Wilson, theorem, if n is a prime number then $a_n = n$, otherwise $a_n = 2$, hence the sequence primality parameter is infinite in this case.