

Alli Fox

Math 115B

HW #3, Section 6.8 #1

The ciphertext 5859 was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$. Using factorization $11413 = 101 \cdot 113$, find the plaintext.

$$\Phi(n) = (p-1)(q-1) = 100 \cdot 112 = 11200$$

We find d such that $de = 1 \pmod{11200}$

Using the extended Euclidean algorithm, we get: $d \equiv e^{-1} \equiv 3 \pmod{11200}$

We now compute $m \equiv c^d \equiv 5859^3 \equiv 1415 \pmod{11413}$