MAT115A HW7

Tao Wang

December 7, 2024

Exercise (1)

Question:

Let $n = 4861$. Use $4860 = 2^2 \cdot 3^5 \cdot 5$ and $x = 11$ to verify that n is prime via Luca's converse of Fermat's Little Theorem or its corollary.

Answer:

Since

$$11^{4860} \equiv 1 (\text{mod } 4861)$$

$$11^{\frac{4860}{2}} \not\equiv 1 (\text{mod } 4861)$$

$$11^{\frac{4860}{3}} \not\equiv 1 (\text{mod } 4861)$$

$$11^{\frac{4860}{5}} \not\equiv 1 (\text{mod } 4861)$$

4861 is prime via Luca's converse of Fermat's Little Theorem.

Exercise (2)

Question:

If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \bmod 26$ are W and B, respectively, then what are the most likely values for a and b?

Answer:

Based on the given information, we can set up the following equations

$$4a + b \equiv 22(\text{mod } 26)$$
$$19a + b \equiv 1(\text{mod } 26)$$

Plug $b \equiv 22 - 4a(\text{mod } 26)$ into the second equation, we get $15a + 22 \equiv 1(\text{mod } 26)$. Then, $15a \equiv -21 \equiv 5(\text{mod } 26)$. Since $15^{-1} \equiv 7(\text{mod } 26)$, $a \equiv 35(\text{mod } 26) = 9$

Plug $a = 9$ back into the first equation, we get $36 + b \equiv 22(\text{mod } 26)$. Therefore, $b \equiv -14 \equiv 12(\text{mod } 26)$.

$\boxed{a = 9}$ and $\boxed{b = 12}$

Exercise (3)

Question:

What is the plaintext message that corresponds to the ciphertex

13 11 11 02

that is produced using modular exponentiation with modulus p = 29 and encryption exponent e = 17?

Answer:

$p = 29$ and $e = 17$.

We have $17d \equiv 1(\text{mod } 28)$ and $d \equiv 5(\text{mod } 28)$

$P \equiv 13^5 \equiv 6(\text{mod } 29)$ and $P \equiv 11^5 \equiv 14(\text{mod } 29)$ and $P \equiv 2^5 \equiv 3(\text{mod } 29)$

Therefore, the plaintext message is 6 14 14 3, or $\boxed{GOOC}$

Exercise (4)

Question:

What is the ciphertext that is produced when RSA encryption with $N = 77$ and $e = 7$ is used to encrypt the message "BEST".

Answer:

BEST = 01 04 18 19

$N = 77$ and $e = 7$

$C \equiv 1^7 \equiv 1(\text{mod } 77)$

$C \equiv 4^7 \equiv 60(\text{mod } 77)$

$C \equiv 18^7 \equiv 39(\text{mod } 77)$

$C \equiv 19^7 \equiv 68(\text{mod } 77)$

Therefore, the ciphertext is $\boxed{01\ 60\ 39\ 68}$.

Exercise (5)

Question:

What is the plaintext message that corresponds to the ciphertext

$$01\ 49\ 49\ 10$$

produced by the RSA encryption with $N = 77$ and $e = 43$.

Answer:

$N = 77$ and $e = 43$

$ed \equiv 1 (\text{mod } \phi(77)) \implies 43d \equiv 1 (\text{mod } 60)$

$d \equiv 7 (\text{mod } 60)$

Therefore, $P \equiv 1^7 \equiv 1 (\text{mod } 77)$ and $P \equiv 49^7 \equiv 14 (\text{mod } 77)$ and $P \equiv 10^7 \equiv 10 (\text{mod } 77)$

The plaintext is 01 14 14 10 or $\boxed{B\ O\ O\ K}$