An RSA Encryption Example and an RSA Decryption Example.

Both examples will use the encryption key (decryption key) \( N = 247 \). The integer \( 247 = 13 \times 19 \), so \( N = pq \) where \( p = 13 \) and \( q = 19 \).

Problem #1 (The Encryption Example)

Using the encryption keys \( N = 247 = 13 \times 19 \) and \( e = 125 = 5^3 \), determine the RSA encryption of the following message.

The message to be encrypted is the single letter "X". Since X is the 24th letter of the alphabet, the code for X is 24.

Solution:

Note: It is not necessary (unless required) to verify that the encryption keys \( N = 247 \) and \( e = 125 \) are appropriate values to use as the keys, but we verify that here for clarity.

The RSA crypto-system requires that, when \( N = pq \) is the product of two primes \( p \) and \( q \), the other key \( e \) must be relatively prime to \( [(p-1)(q-1)] \), that is, \( \gcd(e, [(p-1)(q-1)]) = 1 \).

In this problem, \( N = 13 \times 19 \), so \( (p-1)(q-1) = 12 \times 18 = 216 \).

216 = \( 2^3 \times 3^3 \) and \( e = 125 = 5^3 \) so \( \gcd(125, 216) = 1 \).

\( N = 247 \) and \( e = 125 \) are appropriate as encryption keys.
Here, the message is "X" with a code of 24. This code is the plaintext \( M \) of the message, \( M = 24 \).

The assignment is to find the ciphertext \( C \) of the message. The formula for the ciphertext \( C \) is

\[
C = (M^e \mod N).
\]

Here, for plaintext \( M = 24 \), the formula for the ciphertext is

\[
C = (24^{125} \mod 247).
\]

Expressing the exponent 125 as a sum of powers of 2:

\[
125 = 64 + 32 + 16 + 8 + 4 + 1.
\]

Using the Power Calculator, we find that

\[
24^4 \equiv 55 \pmod{247},
\]

\[
24^8 \equiv 61 \pmod{247},
\]

\[
24^{16} \equiv 16 \pmod{247},
\]

\[
24^{32} \equiv 9 \pmod{247},
\]

\[
24^{64} \equiv 81 \pmod{247},
\]

\[
24^{125} = (24^{64})(24^{32})(24^{16})(24^8)(24^4)(24^1).
\]

By Theorem 8.4.3,

\[
24^{125} \equiv \left[ \frac{(81)(9)(16)(61)(55)(24)}{11,664 \quad 80,520} \right] \pmod{247}
\]

\((81)(9)(16) = 11,664 \) and \((11,664 \mod 247) = 55\)

since \( 11,664 = (247)(47) + 55 \) and \( 0 \leq 55 < 247 \).

\((61)(55)(24) = 80,520 \) and \((80,520 \mod 247) = 245\)

since \( 80,520 = (247)(325) + 245 \) and \( 0 \leq 245 < 247 \).
By Theorem (WIB) 4,
\[ 11,444 \equiv (11,444 \mod 247) \mod 247 \]
and
\[ 80,520 \equiv (80,520 \mod 247) \mod 247. \]

Therefore, by substitution (twice),
\[ (81)(4)(16) \equiv 55 \mod 247 \quad \text{and} \quad (41)(55)(24) \equiv 245 \mod 247. \]

\[ 2^{125} \equiv [(55)(245)] \mod 247. \]

\[ [(55)(245)] \equiv [(55)(245)] \mod 247 \quad \text{by Theorem (WIB) 4.} \]

\[ [(55)(245)] \mod 247 = 137, \quad \text{by a simple calculation.} \]

\[ [(55)(245)] \equiv 137 \mod 247 \quad \text{by substitution.} \]

\[ 2^{125} \equiv 137 \mod 247, \quad \text{by transitivity of "congruence \( \mod 247 \)."} \]

\[ \text{By Theorem 8.4.1, } \quad (2^{125} \mod 247) = (137 \mod 247) = 137. \]

Thus the ciphertext \( C \) for plaintext \( M = 24 \) is \( C = 137 \).
Problem #2 (The Decryption Example).

Using the same value of N, N = 247 = 13 \times 19, and using the fact that the ciphertext C had been generated using the encryption keys N = 247 and e = 125, determine an appropriate decryption key d and then perform RSA decryption of the ciphertext C, where C = 137. Note that ciphertext C = 137 is the ciphertext generated in Problem #1.

Solution: We first determine an appropriate value for the decryption key d.

The RSA cryptosystem requires that the decryption key d must be an inverse of e modulo \( (p-1)(q-1) \), that is d must be a (mod \((p-1)(q-1)\))-inverse of e.

Here, d must be a (mod 216)-inverse of e = 125.

By definition of "(mod 216)-inverse," this means that \((125 \times d) \equiv 1 \pmod{216}\).

Techniques we have studied enable us to discover that d = 197 is a (mod 216)-inverse of 125.

To verify this assertion, note that \((125)(197) = 24,625\)

\[ 24,625 - 1 = 24,624 = (216)(114). \]

\[ 216 \mid (24,625 - 1), \text{ which implies } 24,625 \equiv 1 \pmod{216}. \]

\[ (125)(197) \equiv 1 \pmod{216}. \]

\[ 197 \text{ is a (mod 216)-inverse of 125}. \]

\[ d = 197 \text{ is an appropriate decryption key to use here.} \]
Problem #2 (cont.)

The formula for the decrypted plaintext $M$ given the ciphertext $C$ is

$$M = (C^d \mod N).$$

Here, for ciphertext $C = 137$, the formula for the plaintext is

$$M = (137^{197} \mod 247).$$

(We hope it turns out that $M = 24$, giving the decrypted message "X".)

Now, $197 = 128 + 64 + 4 + 1$.

From the Power Calculator, we have that

$$137^{128} \equiv 16 \pmod{247}$$
$$137^{64} \equiv 61 \pmod{247}$$
$$137^4 \equiv 9 \pmod{247}$$
$$137^1 \equiv 137 \pmod{247}$$

$$137^{197} = (137^{128})(137^{64})(137)^4(137^1)$$

By Theorem 8.4.3,

$$137^{197} \equiv [(16)(61)(9)(137)] \pmod{247}$$

$$(16)(61)(9) = 8784 \text{ and } (8784 \mod 247) = 139$$

Since $8784 = (247)(35) + 139$ and $0 \leq 139 < 247$.

$$[(16)(61)(9)] \equiv 139 \pmod{247}$$

by Theorem (N18) 4 and Substitution (twice).
By Theorem 8.4.5,
\[(16)(41)(9)(137)] \equiv (139)(137) \pmod{247},
\]
\[(139)(137) = 19,043 \text{ and } (19,043 \mod 247) = 24 \]
since \(19,043 = (247)(77) + 24\) and \(0 \leq 24 < 247\).

By Theorem (N18.4) and Substitution,
\[(139)(137) \equiv 24 \pmod{247}\]
\[\Rightarrow [(16)(41)(9)(137) \equiv 24 \pmod{247}] \text{ by Transitivity.} \]
\[\Rightarrow 137 \equiv 24 \pmod{247} \text{ by Transitivity.} \]
\[\Rightarrow (137 \ 197 \mod 247) = (24 \mod 247) = 24 \text{ by Theorem 8.4.1.} \]
\[\Rightarrow \text{For Ciphertext } C = 137, \text{ the decrypted plaintext is } M = 24. \]
The decrypted message is "X".