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 24^{th} 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 $(p-1)(q-1) = 12 \times 18 = 216$.

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

$\therefore N = 247$ 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

$$C = (M^e \bmod N).$$

Here, for plaintext $M = 24$, the formula for the Ciphertext is

$$C = (24^{125} \bmod 247).$$

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

$$24^4 \equiv 55 \pmod{247}$$
$$24^8 \equiv 61 \pmod{247}$$
$$24^{16} \equiv 16 \pmod{247}$$
$$24^{32} \equiv 9 \pmod{247}$$
$$24^{64} \equiv 81 \pmod{247}$$

$$24^{125} = (24^{64})(24^{32})(24^{16})(24^{8})(24^{4})(24^{1}).$$

$\therefore$ By Theorem 8.4.3,

$$24^{125} \equiv [\underbrace{(81)(9)(16)}_{11,664} \underbrace{(61)(55)(24)}_{80,520}] \pmod{247}$$

A simple calculation shows that

$$(81)(9)(16) = (247)(47) + 55$$

$\therefore$ By Theorem 8.4.1, $(81)(9)(16) \equiv 55 \pmod{247}$.

Problem # 1 (cont.)

Another simple calculation shows that

$$(61)(55)(24) = (247)(325) + 245.$$

$\therefore$ By Theorem 8.4.1, $(61)(55)(24) \equiv 245 \pmod{247}$.

Recall that:

① $24^{125} \equiv ((81)(9)(16))((61)(55)(24)) \pmod{247}$

② $(81)(9)(16) \equiv 55 \pmod{247}$

③ $(61)(55)(24) \equiv 245 \pmod{247}$.

$\therefore$ By Theorem 8.4.3, by the transitivity of "Congruence (mod 247)", and by Theorem 8.4.1,

$$24^{125} \equiv (55)(245) \equiv 137 \pmod{247}$$

since $(55)(245) = (247)(54) + 137$.

$\therefore 24^{125} \equiv 137 \pmod{247}$

$(137 \bmod 247) = 137$

since $137 = (247)(0) + 137$
and $0 \leq 137 < 247$.

$\therefore$ By Theorem 8.4.1,

$(24^{125} \bmod 247) = (137 \bmod 247) = 137$

$\therefore (24^{125} \bmod 247) = 137$

$\therefore$ 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 Crypto-system 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 $(125)(197) = 24,625$

$\therefore\ 24,625 - 1 = 24,624 = (216)(114)$.

$\therefore\ 216 \mid (24,625 - 1)$, which implies $24,625 \equiv 1 \pmod{216}$.

$\therefore\ (125)(197) \equiv 1 \pmod{216}$.

$\therefore$ 197 is a (mod 216)-inverse of 125.

$d = 197$ is an appropriate decryption key to use here.

Problem #2 (cont.)

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

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

Here, for ciphertext $C = 137$, the formula for the plaintext is $M = (137^{197} \bmod 247)$.

(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,

$$137^{197} \equiv \Big[\underbrace{(16)(61)}_{976}\underbrace{(9)(137)}_{1,233}\Big] \pmod{247}$$

$(16)(61) \equiv 235 \pmod{247}$ by Theorem 8.4.1 since $(16)(61) = (247)(3) + 235$.

Problem #2 (continued)

To repeat, it was just shown that

$(16)(61) \equiv 235 \pmod{247}$

Now, $(9)(137) \equiv 245 \pmod{247}$ by Theorem 8.4.1

Since $(9)(137) = (247)(4) + 245$.

Recall that $137^{197} \equiv ((16)(61))((9)(137)) \pmod{247}$.

$\therefore$ By Theorem 8.4.3, by transitivity of "congruence (mod 247)" and by Theorem 8.4.1,

$137^{197} \equiv (235)(245) \equiv 24 \pmod{247}$

since $(235)(245) = (247)(233) + 24$.

$\therefore\ 137^{197} \equiv 24 \pmod{247}$.

$(24 \bmod 247) = 24$

since $24 = (247)(0) + 24$ and $0 \le 24 < 247$.

By Theorem 8.4.1, $(137^{197} \bmod 247) = (24 \bmod 247) = 24$.

$\therefore\ (137^{197} \bmod 247) = 24$.

The Plaintext M for Ciphertext $C = 137$ is $M = 24$.

The decrypted message is "X".