Public Key Encryption: Part 1 (for self-study)

1. Write the following composite numbers as a multiplication of their prime factors.

   (a) 72

   (b) 111

   (c) 1024

   (a) $72 = 2^3 \times 3^2$

   (b) $111 = 3 \times 37$

   (c) $1024 = 2^{10}$

2. Complete the following modular arithmetic operations and determine the result:

   (a) $(32 + 18) \bmod 7$

   (b) $(12 \times 8) \bmod 7$

   (c) $(56 + 125) \bmod 11$

   (d) $(33 - 45) \bmod 9$

   (e) $100^4 \bmod 7$

   (f) $7^{-1} \bmod 31$

   (g) $9^{-1} \bmod 19$

   (a) $(32 + 8) \bmod 7$
   $(32 \bmod 7) + (8 \bmod 7) \bmod 7$
   $4 + 1 \bmod 7 = 5$

   (b) $(12 \times 8) \bmod 7$
   $(12 \bmod 7) \times (8 \bmod 7) \bmod 7)$
   $5 \times 1 \bmod 7 = 5$

   (c) $(56 + 125) \bmod 11$
   $(56 \bmod 11) + (125 \bmod 11) \bmod 11$
   $1 + 4 \bmod 11 = 5$

   (d) $(33 - 45) \bmod 9$
   $(33 \bmod 9) - (45 \bmod 9) \bmod 9$
   $6 + 0 \bmod 9 = 6$

   (e) $100^4 \bmod 7 = (100 \bmod 7)^4 \bmod 7$
   $2^4 \bmod 7 = 16 \bmod 7 = 2$

   (f) Since GCD of 31 and 9 is 1 that multiplicative inverse exists. Since $7 * 9 = 63 = 31 \times 2 + 1$ so the inverse is $7^{-1} = 2 \bmod 31$.

   (g) $9 \times (-2) = -18 = 19 - 18 \bmod 19 = 1 \bmod 19$, thus the multiplicative inverse of 9 is -2 which is $19 - 2 = 17$. The answer is 17.

3. Using the "Square and Multiply" modular exponentiation algorithm calculate the following:

   (a) $8^{57} \bmod 11$

   (b) $15^{62} \bmod 31$

(a) Start with MS bit $b_5 = 1$ of $e = 57_{10} = 111001_2$
Set $z = a = 8$ and $n = 11$
$i = 4$: bit $b_4 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 8 * 8^2 \bmod 11 = 6$
$i = 3$: bit $b_3 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 8 * 6^2 \bmod 11 = 2$
$i = 2$: bit $b_2 = 0 \rightarrow$ *square* : z = $z^2 \bmod n = 2^2 \bmod 11 = 4$
$i = 1$: bit $b_1 = 0 \rightarrow$ *square* : z = $z^2 \bmod n = 4^2 \bmod 11 = 5$
$i = 0$: bit $b_0 = 1 \rightarrow$ square multiply: z = $az^2 \bmod n = 8 * 5^2 \bmod 11 = 2$
The answer is 2.

(b) Start with MS bit $b_5 = 1$ of $e = 62_{10} = 111110_2$
Set $z = a = 15$ and $n = 31$
$i = 4$: bit $b_4 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 15 * 15^2 \bmod 31 = 27$
$i = 3$: bit $b_3 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 15 * 27^2 \bmod 31 = 23$
$i = 2$: bit $b_2 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 15 * 23^2 \bmod 31 = 30$
$i = 1$: bit $b_1 = 1 \rightarrow$ square & multiply: z = $az^2 \bmod n = 15 * 30^2 \bmod 31 = 15$
$i = 0$: bit $b_0 = 0 \rightarrow$ *square* : z = $z^2 \bmod n = 15^2 \bmod 31 = 8$
The answer is 8.