Public Key Encryption: Part 1

1. What are the essential ingredients of an asymmetric / public-key cipher?

   - Plaintext: This is the readable message or data that is fed into the algorithm as input.
   - Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
   - Public and private key: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input
   - Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
   - Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

2. What is the difference between the public key and the private key? Why the public-key cryptosystem is still secure even after giving the public key to the attacker?

   The public key is used for the encryption, while the private key (secret key) is used for the decryption. The public key is different from the secret or private key (but related to it).

   It is infeasible for an attacker to deduce the secret key from the public key and the plaintext/ciphertext.

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

   (a) 12

   (b) 78

   (c) 99

   (d) 128

   (a) $12 = 2 \times 2 \times 3 = 2^2 \times 3$

   (b) $78 = 2 \times 3 \times 13$

   (c) $99 = 3 \times 3 \times 11 = 3^2 \times 11$

   (d) $128 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^7$

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

   (a) $(12 + 8) \bmod 6$

   (b) $(2 \times 12) \bmod 6$

   (c) $(20 + 125) \bmod 5$

   (d) $(20 - 35) \bmod 5$

   (e) $10^4 \bmod 3$

   (f) $10^{-1} \bmod 31$

   (g) $13^{-1} \bmod 19$

   (a) $(12 + 8) \bmod 6 = 2$

   (b) $(2 \times 12) \bmod 6 = 0$

(c) $(20 + 125) \bmod 5 = 0$

(d) $(20 - 35) \bmod 5 = 0$

(e) $10^4 \bmod 3 = (10 \bmod 3)^4 \bmod 3 = 1^4 \bmod 3 = 1$ alternatively $10^4 \bmod 3 = (9999 + 1) \bmod 3 = 1$

(f) Since GCD of 31 and 10 is 1 that multiplicative inverse exists. Since $31 = 10 * 3 + 1$ so $1 = 31 + 10(-3)$. By taking modulus at both sides, $1 = 10 * (-3) \bmod 31$. The inverse is $-3 \bmod 31$ i.e. $28 \bmod 31$.

(g) $13 * 3 \bmod 19 = 39 \bmod 19 = 1$, thus the multiplicative inverse of 13 is 3.

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

(a) $71^{56} \bmod 11$

(b) $58^{66} \bmod 31$

(a) Start with MS bit $b_5 = 1$ of $e = 56_{10} = 111000_2$ and since $71 = 5 \bmod 11$
Set $z = a = 5$ and $n = 11$
$i = 4$: bit $b_4 = 1 \rightarrow$ square & multiply: $\mathrm{z} = \mathrm{az}^2 \bmod n = 5 * 25 \bmod 11 = 4$
$i = 3$: bit $b_3 = 1 \rightarrow$ square & multiply: $\mathrm{z} = \mathrm{az}^2 \bmod n = 5 * 4^2 \bmod 11 = 3$
$i = 2$: bit $b_2 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 3^2 \bmod 11 = 9$
$i = 1$: bit $b_1 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 9^2 \bmod 11 = 4$
$i = 0$: bit $b_0 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 4^2 \bmod 11 = 5$
The answer is 5.

(b) Start with MS bit $b_6 = 1$ of $e = 66_{10} = 1000010_2$ and since $58 = 27 \bmod 31$
Set $z = a = 27$ and $n = 31$
$i = 5$: bit $b_5 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 27^2 \bmod 31 = 16$
$i = 4$: bit $b_4 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 16^2 \bmod 31 = 8$
$i = 3$: bit $b_3 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 8^2 \bmod 31 = 2$
$i = 2$: bit $b_2 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 2^2 \bmod 31 = 4$
$i = 1$: bit $b_1 = 1 \rightarrow$ square & multiply: $\mathrm{z} = \mathrm{az}^2 \bmod n = 27 * 4^2 \bmod 31 = 29$
$i = 0$: bit $b_0 = 0 \rightarrow$ *square* $: \mathrm{z} = \mathrm{z}^2 \bmod n = 29^2 \bmod 31 = 4$
The answer is 4.