German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Practice Assignment 3

Discussion 22/02/2020 - 27/02/2020

---

1 RSA Encryption

Perform encryption using the RSA algorithm, for the following:

1. p = 3; q = 11, e = 7; M = 5

Solution: $n = p * q = 3 * 11 = 33$
$C = M^e \bmod n = 5^7 \bmod 33 = 14$

2. p = 5; q = 17, e = 3; M = 9

Solution: $n = p * q = 5 * 17 = 85$
$C = M^e \bmod n = 9^3 \bmod 85 = 49$

3. p = 7; q = 5, d = 17; M = 8, (Encrypt using Private-Key)

Solution: $n = p * q = 7 * 5 = 35$
$C = M^d \bmod n = 8^{17} \bmod 35 = 8$

2 RSA Decryption

Perform decryption using the RSA algorithm, for the following:

1. p = 11; q = 13, e = 11; C = 106

Solution: $n = p * q = 11 * 13 = 143$
$\Phi(n) = (p - 1)(q - 1) = 10 * 12 = 120$
Now we have $e = 11$ and $\Phi(n) = 120$, we know that

$$e * d = 1 + k * \Phi(n)$$
$$11 * d = 1 + k * 120,$$

using the Euclidean algorithm we calculate by:

$$120 = 11(10) + 10$$
$$11 = 10(1) + 1$$

Write that last one as:

$$1 = 11 - 10(1)$$

Now substitute the first equation into 10:

$$1 = 11 - (120 - 11(10))$$

Note that this is a linear combination of 120 and 11, after simplifying we get:

$$1 = 11 - 120 + 11(10)$$
$$1 = 11(1 + 10) - 120$$
$$1 = 11(11) - 120$$
$$1 + 120 = 11(11)$$

We get $k = 1$ and $d = 11$

$$\mathbf{M = C^d \bmod n = 106^{11} \bmod 143}$$
$$= (\mathbf{106^4 \bmod 143 * 106^4 \bmod 143 * 106^3 \bmod 143}) \bmod \mathbf{143}$$
$$= (\mathbf{3 * 3 * 112}) \bmod \mathbf{143 = 7}$$

2. p = 17; q = 31, e = 7; C = 128

Solution: $n = p * q = 17 * 31 = 527$
$\Phi(n) = (p-1)(q-1) = 16 * 30 = 480$
Now we have $e = 7$ and $\Phi(n) = 480$, we know that

$$e * d = 1 + k * \Phi(n)$$
$$7 * d = 1 + k * 480,$$

using the Euclidean algorithm we calculate by:

$$480 = 7(68) + 4$$
$$7 = 4(1) + 3$$
$$4 = 3(1) + 1$$

Write that last one as:

$$1 = 4 - 3(1)$$

Now substitute the second equation into 3:

$$1 = 4 - (7 - 4(1))$$

Then we substitute the first equation into every instance of 4:

$$1 = (480 - 7(68)) - (7 - (480 - 7(68))(1))$$

Note that this is a linear combination of 480 and 7, after simplifying we get:

$$\begin{gathered}1 = 480 - 7(68) - 7 + 480 - 7(68) \\ 1 = 480(2) - 7(137) \\ 1 - 480(2) = -7(137) \\ 1 + 480(-2) = 7(-137)\end{gathered}$$

We get $k = -2$ and $d = -137$ which is in fact 343 mod 480 since -137 + 480 = 343
so d = 343

$$\begin{gathered}\mathbf{M} = \mathbf{C^d} \bmod \mathbf{n} = \mathbf{128^{343}} \bmod \mathbf{527} \\ = ((\mathbf{128^{256}} \bmod \mathbf{527}) * \mathbf{128^{64}} \bmod \mathbf{527} * \mathbf{128^{16}} \bmod \mathbf{527} \\ *\mathbf{128^{4}} \bmod \mathbf{527} * \mathbf{128^{1}} \bmod \mathbf{527}) \bmod \mathbf{527} \\ = (\mathbf{35} * \mathbf{256} * \mathbf{35} * \mathbf{101} * \mathbf{47} * \mathbf{128}) \bmod \mathbf{527} = \mathbf{2}\end{gathered}$$

3. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is (e = 5, n = 35). What is the plaintext M?

Solution: By trial and error we try to find two prime numbers whose multiplication is equal to 35, we get;

$$\begin{gathered}\mathbf{p} = 7 \\ \mathbf{q} = 5\end{gathered}$$

we then calculate $\Phi(n)$

$$\Phi(n) = (p-1)(q-1) = 6 * 4 = 24$$

Now we have $e = 5$ and $\Phi(n) = 24$, we know that

$$\begin{gathered}e * d = 1 + k * \Phi(n) \\ 5 * d = 1 + k * 24,\end{gathered}$$

using the Euclidean algorithm we calculate by:

$$\begin{gathered}24 = 5(4) + 4 \\ 5 = 4(1) + 1\end{gathered}$$

Write that last one as:

$$1 = 5 - 4(1)$$

Now substitute the first equation into 4:

$$1 = 5 - (24 - 5(4))$$

Note that this is a linear combination of 24 and 5, after simplifying we get:

$$\begin{gathered} 1 = 5 - 24 + 5(4) \\ 1 = 5(1 + 4) - 24 \\ 1 = 5(5) - 24 \\ 1 + 24 = 5(5) \end{gathered}$$

We get $k = 1$ and $d = 5$

$$\mathbf{M} = \mathbf{C^d} \bmod \mathbf{n} = \mathbf{10^5} \bmod \mathbf{35} = \mathbf{5}$$

4. p = 7; q = 11, e = 7; C = 59

Solution: $n = p * q = 7 * 11 = 77$
$\Phi(n) = (p-1)(q-1) = 6 * 10 = 60$
Now we have $e = 7$ and $\Phi(n) = 60$, we know that

$$\begin{gathered} e * d = 1 + k * \Phi(n) \\ 7 * d = 1 + k * 60, \end{gathered}$$

using the Euclidean algorithm we calculate by:

$$\begin{gathered} 60 = 7(8) + 4 \\ 7 = 4(1) + 3 \\ 4 = 3(1) + 1 \end{gathered}$$

Write that last one as:

$$1 = 4 - 3(1)$$

Now substitute the second equation into 3:

$$1 = 4 - (7 - 4(1))(1)$$

Now substitute the first equation into every instance of 4:

$$1 = (60 - 7(8)) - (7 - (60 - 7(8))(1))(1)$$

Note that this is a linear combination of 60 and 7, after simplifying we get:

$$1 = 60 - 7(8) - 7 + 60 - 7(8)$$
$$1 = 60(2) - 7(8 + 8 + 1)$$
$$1 = 60(2) - 7(17)$$
$$1 - 60(20) = -7(17)$$
$$1 + 60(-2) = 7(-17)$$

We get $k = -2$ and $d = -17$ which is in fact 43 mod 60 since -17 + 77 = 60
so d = 43

$$\mathbf{M} = \mathbf{C^d} \bmod \ \mathbf{n} = \mathbf{59^{43}} \bmod \ \mathbf{77}$$
$$= ((\mathbf{59^5} \bmod \ \mathbf{77})^{\mathbf{8}} * \mathbf{59^2} \bmod \ \mathbf{77}) \bmod \ \mathbf{77} = \mathbf{31}$$

5. In an RSA system, Alice's public key is e, n = 5, 851. Discover the corresponding private key.

Solution: By trial and error we try to find two prime numbers whose multiplication is equal to 851, we get;

$$\mathbf{p} = 23$$
$$\mathbf{q} = 37$$

we then calculate $\Phi(n)$

$$\Phi(n) = (p - 1)(q - 1) = 22 * 36 = 792$$

Now we have $e = 5$ and $\Phi(n) = 792$, we know that

$$e * d = 1 + k * \Phi(n)$$
$$5 * d = 1 + k * 792,$$

using the Euclidean algorithm we calculate by:

$$792 = 5(158) + 2$$
$$5 = 2(2) + 1$$

Write that last one as:

$$1 = 5 - 2(2)$$

Now substitute the first equation into 2:

$$1 = 5 - 2(792 - 5(158))$$

Note that this is a linear combination of 792 and 5, after simplifying we get:

$$1 = 5 - 792(2) + 5(316)$$
$$1 = 5(1 + 316) - 792(2)$$
$$1 = 5(317) - 792(2)$$
$$1 + 792(2) = 5(317)$$

We get $k = 2$ and $d = 317$