Fundamentals of Cryptography

Homework 5

Sepehr Ebadi 9933243

Question 1

1)

$$
\begin{array}{l}
p = 751, \alpha = 3, KprB = 123, i = KprA \; = 320, x = 71 \\
KpubB = \; \alpha^{KprB} \; mod \; p \\
KpubA = \; \alpha^{i} \; mod \; p \\
KM = \; KpubB^{i} \; mod \; p \\
Encrypted = y = x \ast KM \; mod \; p \\
Decrypted = x = y \ast \; KM^{-1} \; mod \; p
\end{array}
$$

$$
\begin{array}{l}
KpubB = \; 3^{123} \; mod \; 751 = 743 \\
KpubA = \; 3^{320} \; mod \; 751 = 378 \\
KM = \; 743^{320} \; mod \; 751 = 499 \\
y = 71 \ast 499 \; mod \; 751 = 132 \\
x = 132 \ast 450 \; mod \; 751 = 71
\end{array}
$$

2)

$$
\begin{array}{l}
p = 751, \alpha = 3, KprB = 123, i = KprA \; = 210, x = 45 \\
KpubB = \; \alpha^{KprB} \; mod \; p \\
KpubA = \; \alpha^{i} \; mod \; p \\
KM = \; KpubB^{i} \; mod \; p \\
Encrypted = y = x \ast KM \; mod \; p \\
Decrypted = x = y \ast \; KM^{-1} \; mod \; p
\end{array}
$$

$$
\begin{array}{l}
KpubB = \; 3^{123} \; mod \; 751 = 743 \\
KpubA = \; 3^{210} \; mod \; 751 = 485 \\
KM = \; 743^{210} \; mod \; 751 = 51 \\
y = 45 \ast 51 \; mod \; 751 = 42 \\
x = 42 \ast 162 \; mod \; 751 = 45
\end{array}
$$

3)

$$
\begin{array}{l}
p = 751, \alpha = 3, KprB = 500, i = KprA \; = 120, x = 500 \\
KpubB = \; \alpha^{KprB} \; mod \; p \\
KpubA = \; \alpha^{i} \; mod \; p \\
KM = \; KpubB^{i} \; mod \; p \\
Encrypted = y = x \ast KM \; mod \; p
\end{array}
$$

$$Decrypted = x = y * \ KM^{-1} \, mod \, p$$

$$
\begin{aligned}
&KpubB = \ 3^{500} \, mod \, 751 = 72 \\
&KpubA = \ 3^{120} \, mod \, 751 = 556 \\
&KM = \ 72^{120} \, mod \, 751 = 1 \\
&y = 500 * 1 \, mod \, 751 = 500 \\
&x = 500 * 1 \, mod \, 751 = 500
\end{aligned}
$$

Question 2

1)

$$n = 11$$

$$\alpha = 2, p = 2{,}5, \emptyset(11) = 10$$

$$p = 5 \rightarrow \ 2^{\frac{10}{5}} = 4 \, mod \, 11 \neq 1$$

$$p = 2 \rightarrow 2^{\frac{10}{2}} = 32 \, mod \, 11 = 10 \neq 1$$

پس نتیجه می گیریم ۲ یک مولد برای ۱۱ می باشد.

2)

$$n = 11^2$$

$$\alpha = 2, p = 2{,}5{,}11, \emptyset(11^2) = 110$$

$$p = 5 \rightarrow \ 2^{\frac{110}{5}} = 81 \, mod \, 11^2 \neq 1$$

$$p = 2 \rightarrow 2^{\frac{110}{2}} = 120 \, mod \, 11^2 \neq 1$$

$$p = 11 \rightarrow 2^{\frac{110}{11}} = 56 \, mod \, 11^2 \neq 1$$

پس نتیجه می گیریم ۲ یک مولد برای 11^2 می باشد.

3)

$$n = 2 * 11^2$$

$$\alpha = 2, p = 2{,}5{,}11, \emptyset(2 * 11^2) = 110$$

$$p = 5 \rightarrow \ 2^{\frac{110}{5}} = 202 \, mod \, 2 * 11^2 \neq 1$$

$$p = 2 \rightarrow 2^{\frac{110}{2}} = 120 \, mod \, 2 * 11^2 \neq 1$$

$$p = 11 \rightarrow 2^{\frac{110}{11}} = 56 \, mod \, 2 * 11^2 \neq 1$$

پس نتیجه می گیریم ۲ یک مولد برای $2 * 11^2$ می باشد.

4)

$$n = 11^{100}$$

$$\alpha = 2, p = 2{,}5{,}11, \emptyset(11^{100}) = 12527829 \ldots$$

$$p = 5 \rightarrow \ 2^{\frac{12527829\ldots}{5}} = \cdots \, mod \, 11^{100} \neq 1$$

$$p = 2 \rightarrow 2^{\frac{12527829\ldots}{2}} = \cdots \, mod \, 11^{100} \neq 1$$

$$p = 11 \rightarrow 2^{\frac{12527829\ldots}{11}} = \cdots \; mod\; 11^{100} \neq 1$$

پس نتیجه می گیریم ۲ یک مولد برای 11^{100} می باشد.

Question 3

$$\begin{gathered} p = 44927, \alpha = 7, d = KprB = 22105, m = 10101 \\ KpubB = \; \alpha^{d}\; mod\; p = 7^{22105}\; mod\; 44927 = 40909 \end{gathered}$$

در این جا باید i را انتخاب کنیم که به صورت تصادفی بین ۲ تا p-2 انتخاب میکنیم :

$$\begin{aligned} & i = 32 \\ & KE = KpubA = \alpha^{i}\; mod\; p = \; 7^{32}\; mod\; p = 44755 \\ & KM = KpubB^{i}\; mod\; p = 10600 \\ & Encryption = y = x * KM\; mod\; p = 10101 * 10600\; mod\; p = 9559 \\ & Decryption = x = y * KM^{-1}\; mod\; p = 9559 * 23468\; mod\; p = 10101 \end{aligned}$$

Question 4

1)

$$\begin{gathered} x = 0 \rightarrow y^{2} = 0^{3} + (3 * 0) + 2 = 2\; mod\; 7 \rightarrow 3{,}4 \\ x = 1 \rightarrow y^{2} = 1^{3} + (3 * 1) + 2 = 6\; mod\; 7 \rightarrow \times \\ x = 2 \rightarrow y^{2} = 2^{3} + (3 * 2) + 2 = 2\; mod\; 7 \rightarrow 3{,}4 \\ x = 3 \rightarrow y^{2} = 3^{3} + (3 * 3) + 2 = 3\; mod\; 7 \rightarrow \times \\ x = 4 \rightarrow y^{2} = 4^{3} + (3 * 4) + 2 = 1\; mod\; 7 \rightarrow 1{,}6 \\ x = 5 \rightarrow y^{2} = 5^{3} + (3 * 5) + 2 = 2\; mod\; 7 \rightarrow 3{,}4 \\ x = 6 \rightarrow y^{2} = 6^{3} + (3 * 6) + 2 = 5\; mod\; 7 \rightarrow \times \end{gathered}$$

$$\{(0{,}3), (0{,}4), (2{,}3), (2{,}4), (4{,}1), (4{,}6), (5{,}3), (5{,}4)\}$$

2)

$$E = \{0, (0{,}3), (0{,}4), (2{,}3), (2{,}4), (4{,}1), (4{,}6), (5{,}3), (5{,}4)\} = 9$$

3)

$$\begin{gathered} 0 * a = 0 \\ 1 * a = (0{,}3) \\ 2 * a = (2{,}3) \\ 3 * a = (5{,}4) \\ 4 * a = (4{,}6) \\ 5 * a = (4{,}1) \end{gathered}$$

$$6 * a = (5,3)$$
$$7 * a = (2,4)$$
$$8 * a = (0,4)$$
$$9 * a = 0$$
$$|a| = 9 = E$$

پس نتیجه می گیریم که a یک مولد است.

Question 5

$k = 13, p = (6,3), Q = \sigma$

$\mathbf{1}) \boldsymbol{k\ is\ odd}$:

$Q + N = Q = (6,3)$

$m = \dfrac{3.6^2 + 2}{2.3}\ mod\ 17 = \dfrac{110}{6}$

$6^{-1}\ mod\ 17 = 3 \rightarrow m = (3.110) mod\ 17 = 7$

$x3 = (7^2 - 6 - 6)\ mod\ 17 = 3, y3 = (7.(6 - 3) - 3) mod\ 17 = 1 \rightarrow\ N = (3,1)$

$k = 6, Q = (6,3), N = (3,1)$

$\mathbf{2}) \boldsymbol{k\ is\ even}$:

$m = \dfrac{3.3^2 + 2}{2.1}\ mod\ 17 = 6$

$x3 = (6^2 - 3 - 3) mod\ 17 = 13, y3 = (6.(3 - 13) - 1) mod\ 17 = 7 \rightarrow N = (13,7)$

$k = 3, Q = (6,3), N = (13,7)$

$\mathbf{3}) \boldsymbol{k\ is\ odd}$:

$m = \dfrac{7 - 3}{13 - 6}\ mod\ 17 = \dfrac{4}{7}$

$7^{-1}\ mod\ 17 = 5 \rightarrow m = (4.5) mod\ 17 = 3$

$x3 = (3^2 - 6 - 13) mod\ 17 = 7, y3 = (3.(6 - 7) - 3) mod\ 17 = 11 \rightarrow Q = (7,11)$

$m = \dfrac{3.13^2 + 2}{2.7}\ mod\ 17 = \dfrac{511}{14}$

$14^{-1}\ mod\ 17 = 11 \rightarrow m = (511.11) mod\ 17 = 6$

$x3 = (6^2 - 13 - 13)\ mod\ 17 = 10, y3 = (6.(13 - 10) - 7) mod\ 17 = 11 \rightarrow N = (10,11)$

$k = 1, Q = (7,11), N = (10,11)$

$\mathbf{4}) \boldsymbol{k\ is\ odd}$:

$m = \dfrac{11 - 11}{10 - 7}\ mod\ 17 = 0$

$x3 = (0^2 - 7 - 10) mod\ 17 = 0, y3 = (0.(7 - 0) - 11) mod\ 17 = 6 \rightarrow Q = (0,6)$

$k = 0, Q = (0,6)$

$=> 13p = (0,6)$

Question 6

$\text{private key} = \alpha = 6, \text{KpubB} = B = (5{,}9), y^2 \equiv x^3 + x + 6 \bmod 11$

$K = 6 * B = 2(2B + B)$

$2B = (X3, Y3), X1 = X2 = 5, Y1 = Y2 = 9$

$s = (3X1^2 + a) * 2Y1^{-1} \bmod 11 = 3 \bmod 11$

$X3 = s^2 - X1 - X2 \bmod 11 = 10 \bmod 11$

$Y3 = s(X1 - X3) - Y1 \bmod 11 = 9 \bmod 11 \rightarrow 2B = (10{,}9)$

$3B = 2B + B = (X3', Y3'), X1 = 10, X2 = 5, Y1 = Y2 = 9$

$s = (Y1 - Y2)(X2 - X1)^{-1} \bmod 11 = 0 \bmod 11$

$X3' = s^2 - X1 - X2 \bmod 11 = 7 \bmod 11$

$Y3' = s(X1 - X3') - Y1 \bmod 11 = 2 \bmod 11 \rightarrow 3B = (7{,}2)$

$6B = 2 * 3B = \left(X3'', Y3''\right), X1 = X2 = 7, Y1 = Y2 = 2$

$s = (3X1^2 + a) * 2Y1^{-1} \bmod 11 = 4 \bmod 11$

$X3'' = s^2 - X1 - X2 \bmod 11 = 2 \bmod 11$

$Y3'' = s\left(X1 - X3''\right) - Y1 \bmod 11 = 7 \bmod 11 \rightarrow 6B = (2{,}7)$

$KAB = X3'' = 2$