Qutaiba ALASHQAR, 20290036.

Bilgi güvenliği sınavı, 27. 04. 2023.

1. soru //

Diffie-Hellman anahtarına göre, $P = 73$, $\alpha = 3$, $a = 5$, $b = 7$

Ortak anahtarı ?

$K_{pubA} = (\alpha^{a}) \pmod{p}$

$K_{pubB} = (\alpha^{b}) \pmod{p}$

$K_{pubA} = 3^{5} \pmod{73} \Rightarrow K_{pubA} = \boxed{24} \longrightarrow$ bunu B'ye gönderiyoruz

$K_{pubB} = 3^{7} \pmod{73} \Rightarrow K_{pubB} = \boxed{} \longrightarrow$ A'ye gönderiyoruz
70

$K_A = (B\text{ nın değeri})^{a} \pmod{p} \Rightarrow K_A = 70^{5} \pmod{73} = 49$

$K_B = (A\text{ nın değeri})^{b} \pmod{p} \Rightarrow K_B = 24^{7} \pmod{73} = 49$

ortak key $= 62$

2. Soru//

$GF(2^8)$, $(x^7+x^5+x^3+x) * (x^5+x^3+x^2+x)$

$P(x) = x^8+x^4+x^3+x+1$

$A(x).B(x) = C'(x)$ $B = x^5+x^3+x^2+x$

$c'(x) = ?$

$x^7+x^5+x^3+x \Rightarrow$ ~~0101010~~ 10101010 ~~te~~ right shift

$x^5+x^3+x^2+x \Rightarrow 00101110$ left shift

$01010101 \Rightarrow x^6+x^4+x^2+1 \rightarrow A$

$01011100 \Rightarrow x^6+x^5+x^4+x^3 \rightarrow B$

~~B =~~

$\boxed{B = x^6+x^2+x}$

$00101010 \Rightarrow x^5+x^3+x$

$10111000 \Rightarrow x^7+x^5+x^4+x^3$ $B = x^7+x^6+x^5+x^4+x^3+x^2+1$

$00010101 \Rightarrow x^4+x^2+1$

$01110000 \Rightarrow x^6+x^5+x^4$ $B = x^7+x^3+x^2+1$

$00001010 \Rightarrow x^3+x^2$

$11100000 \Rightarrow x^7+x^6+x^5$ $B = x^6+x^5+x^3+x^2+1$

$00000101 \Rightarrow x^2+1$

$11000000 \Rightarrow x^7+x^6$ $B = x^7+x^5+x^3+x^2+1$

$00000010 \Rightarrow x$

$10000000 \Rightarrow x^7$ $B = x^5+x^3+x^2+1$

$00000000 \Rightarrow 1$ ✓

$00000000 \Rightarrow 1$

$\boxed{B = x^5+x^3+x^2}$

$C(x) = x^5+x^3+x^2$

← 2.

$C'(x) = x^5 + x^3 + x^2$

$P(x) = x^8 + x^4 + x^3 + x + 1$

$= (x^5 + x^3 + x^2) \ (\mathrm{mod}\ x^8 + x^4 + x^3 + x + 1)$

$x^8 = 1 . p(x) + (x^4 + x^3 + x + 1)$

$x^9 = x^5 + x^4 + x^2 + x + x^5 + x^3 + x^2$

$= \boxed{x^4 + x^3}$ ← cevap

3. Soru// oneTpad

Açık metin 1010 1010 1010
Şifreli metin 1111 1111 0000

Anahtar//

One pad, XOR kullanarak on yapılır $e_{k_i}(x_i) = x_i \oplus k_i$

Açık metin 1010 1010 1010
Şifreli ise 1111 1111 0000

0101 0101 1010

→ Üç tane anahtar ürettik 4 bitlik

⊕XOR		
0	0	0
0	1	1
1	0	1
1	1	0

Anahtarımız $\boxed{0101\ 0101\ 1010}$

4. soru//

13 sayı mod 37, tersini extended Euclidean ile.

$\overset{r_0}{37} = 2\cdot\overset{r_1}{13} + \overset{r_2}{11}$

$\overset{r_1}{13} = 1\cdot\overset{r_2}{11} + \overset{r_3}{2}$

$\overset{r_2}{11} = 5\cdot\overset{r_3}{2} + \overset{r_4}{\boxed{1}}$

~~$\overset{r_3}{2} = 2\cdot\overset{r_4}{1} + \overset{r_5}{0}$~~ ← X

$r_2 = r_0 - 2r_1$

$r_3 = r_1 - r_2$

$= r_1 - r_0 + 2r_1$

$= 3r_1 - r_0$

$r_4 = r_2 - r_3$

$r_4 = r_0 - 2r_1 - 3r_1 + r_0$

$= 2r_0 - \cancel{5}r_1$

$1 = 11 - 5\times 2$

$= (6)(11) - (5)(13)$

$= (6)(37) - (17)(13)$

$-221 = (\text{mod } 37)$

Şimdi $-221 = 1 (\text{mod } 37)$

$-(17)(13) = \text{mod } 37$

$37 - 17 = \boxed{20}$

Invers Eu. $\boxed{20} \rightarrow r^{-1}$

5. Soru//

111000 tabloya göre //

$(0011\ 1000)_2 \rightarrow x^5+x^4+x^3.$

↳ 16 decimal $\Rightarrow (38)_{16}$

$(38)_{16} \Rightarrow$ tablordan ise $\rightarrow (06)_{tablo}$

$(06)_{16} \rightarrow (00000110)_2$

$0000\ 0110 \Rightarrow x^2+x$

6./soru 11

Square and Multiply alg.

$2^{43} \bmod 97 = ?$

ilk adım $(43)_{10} \rightarrow (101011)_2 \Rightarrow (0010\ 1011)_2 \Rightarrow$
$(h_5, h_4, h_3, h_2, h_1, h_0)$

i			
0	1	1	2
1	10	x	4
2	101	x^2+1	16
3	1010	x^3+x	62
4	10101	x^4+x^2+1	61
5	101011	x^5+x^3+x+1	35
6	~~101011~~		

$a^{\text{pow} 2} (\bmod p)$

$2 (\bmod 97) = 2$

$4 (\bmod 97) = 4$

$16 (\bmod 97) = 16$

$256 (\bmod 97) = 62$

$3844 (\bmod 97) = 61$

$3721 (\bmod 97) = 35$

~~2 4 16 26 61~~ 35

~~1 0 1 0~~ 1 0

35	61	62	16	4	2
1	0	1	0	1	1

$35 \times 62 \times 4 \times 2 \Rightarrow 17360 \bmod 97$

$= \boxed{94}$

7.