Qutaiba ALASHQAR, 20290036. Bilgi gavenligi sınavı, 27.04.2023.

1. som //

Diffie-Hellman anahm gone, P=73, ==3, a=5, b=7

Ortak anuhtan?

 $k \operatorname{pub} A = (\alpha^9) (\operatorname{mod} P)$ $k \operatorname{pub} B = (\alpha^9) (\operatorname{mod} P)$

KpubA = 35 (mod 73) => KpubA = bunu Blye ginhungaruz

tpubB= 37 (mod 73) => KpubB= A'ye gindungaruz

70

K A = (B mindegre) a (mod P) => KA = 70 0 0 5 (mod 73) = 49 49

KB = (A mod p) => KB = 247 (mod 73) = 49

ortak key = 62



2. son4// GF(2), (x2+x5+x3+x) x (x5+x3+x2+x) P(x)= x + x + x + x + x + 1 B= 25+27+22+2 A(x). B(x) = C'(x)c'(x) =? 4x2+ 23+x => otolol 10101010 1 might ship lest ships 23+ 23+ 22+2 => 00101110 01010101 => x + x + x + 1 >A + 01011100 => x6+ x5+ x4+ x3 -> B B= x6+x2+ 2 00101010 => x3+x3+x B= x+ x6+ x5+ x+ x+ x+ 1 10111000 => 27+ 25+ 24+ 23 000 10101=> x4, x2+1 $13 = \chi^{7} + \chi^{3} + \chi^{2} + 1$ 0111 0000 => 26+25+24 0000 lolo=> x3+ x2 B = x6+ x5+ x3+ x2+1 11100000=> 77+26+25 00000 |01=) 22+1 B = x7 + x5 + x2 + x2+1 1 1000000 => 27+26 0 00000 0 lo => x 13 = x5+x3+x2+1 100000000=> 27 00000000=>1V B= x3+x3+x2 0 0000000 31 C(x)= x5+ x3+x2 (2.)

 $C'(x) = \chi^{5} + \chi^{3} + \chi^{2}$ $P(x) = \chi^{8} + \chi^{4} + \chi^{3} + \chi^{+1}$ $= (\chi^{5} + \chi^{3} + \chi^{2}) \pmod{\chi^{8} + \chi^{4} + \chi^{3} + \chi^{+1}}$ $\chi^{8} = 1 \cdot p(\chi) + (\chi^{4} + \chi^{3} + \chi^{+1})$ $\chi^{8} = \chi^{5} + \chi^{4} + \chi^{2} + \chi + \chi^{5} + \chi^{3} + \chi^{2}$ $= \chi^{4} + \chi^{2} + \chi^{4} + \chi^{2} + \chi^{4} + \chi^{5} + \chi^{3} + \chi^{2}$ $= \chi^{4} + \chi^{2} + \chi^{4} + \chi^{2} + \chi^{4} + \chi^{5} +$

3. Sorul/ onexpad

Agik mesim 1010 lolo lolo

Sifreti mesim 1111 1111 0000

Anathrow//

One pad, 20R kallowsk on yapılır (2ki(2i) - 2i) (2) ki

Agik mesim lolo lolo lolo

Sifreti ise 1111 1111 0000

OxoR | Ololo101 | Olo

Ololo101 | Olo

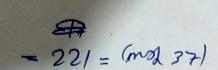
Araktowinz | Olol 0101 | Olo

Araktowinz | Olol 0101 | Olo

4.

4.50mu//
13 say, mod 37, torsini ettemded fuclidens ile.

$$r_2 = r_0 - 2r_1$$
 $r_3 = r_1 - r_2$
 $= r_1 - r_0 + 2r_1$
 $= 3r_1 - r_0$
 $r_4 = r_2 - r_3$
 $r_4 = r_0 - 2r_1 - 3r_1 + r_0$
 $= 2r_0 - \frac{r_0}{r_0}$



$$1 = 11 - 512$$

$$= (6)(1) - (5)(13)$$

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





6. / soru 11

Square and Multiply alg.

2 mod 97 =?

ilk ahm (43)10 -> (101011)2 => (00101011)2 => (h5, hy, h3, h2h1, h0)

i	B. S. T.		
0		20 1	2
T	10	20	Ч
2	101	2 2 2 1	(6
3	1010	28+ 2°	62
14	10101	オナンナノ	61
5	101011	x5+x7+2+1	35
6	101011		

2 (mode) 2 (mode) 2 (mode) 4 (mod 97) = 2 4 (mod 97) = 4 (6 (mod 97) = 16 2 56 (mod 97) = 62 3844 (mod 97) = 61 3721 (mod 97) = 35

35 x 62 x 4 x 2

