Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ

Практическая работа №4

Создание ключей в системе PGP, передача подписанных и защищенных сообщений

Проверил:
Давыдович К. И.

Выполнили:
Мисевич А. С.

Минск 2023

Цель работы

Исследование ассиметричных алгоритмов шифрования.

Задача

Переведите число 3^{43} в двоичную систему счисления.

Найдите состояние 28-разрядного двоичного регистра сдвига после циклического сдвига влево на 5, числа **X**, предварительно записанного в регистр.

вариант	X	вариант	X	вариант	X
1	179317333_{10}	2	179316333_{10}	3	119317333_{10}
4	479317333_{10}	5	179327333_{10}	6	129317333_{10}
7	579317333_{10}	8	179337333_{10}	9	139317333_{10}
10	679317333_{10}	11	179357333_{10}	12	149317333_{10}
13	779317333_{10}	14	179117333_{10}	15	159317333_{10}
16	179317353_{10}	17	179217333_{10}	18	179317333_{10}
19	179317133_{10}	20	179517333_{10}	21	279317333_{10}
22	179317233_{10}	23	179717333_{10}	24	379317333_{10}
25	179317533_{10}	26	171317333_{10}	27	179317331_{10}
28	179311333_{10}	29	172317333_{10}	30	179317332_{10}
31	179312333_{10}	32	177317333_{10}	33	179317313_{10}
34	179317333_{10}	35	175317333_{10}	36	179317323_{10}

Найдите сумму по модулю 2 двух чисел 2244899301_{10} и **X**.

Вариант 14

Задание 1

1) 3^43 / 2 = 16412848369726853881З (ост. 1)
2) 16412848369726853881З / 2 = 8206424184863426940б (ост. 1)
3) 8206424184863426940б / 2 = 4103212092431713470З (ост. 0)
4) 4103212092431713470З / 2 = 2051606046215856735І (ост. 1)
5) 2051606046215856735І / 2 = 1025803023107928367З (ост. 1)
6) 1025803023107928367З / 2 = 5129015115539641837 (ост. 1)
7) 5129015115539641837 / 2 = 2564507557769820918 (ост. 1)
8) 2564507557769820918 / 2 = 1282253778884910459 (ост. 0)
9) 1282253778884910459 / 2 = 641126889442455229 (ост. 1)
10) 641126889442455229 / 2 = 320563444721227614 (ост. 1)
11) 320563444721227614 / 2 = 160281722360613807 (ост. 0)
12) 160281722360613807 / 2 = 80140861180306903 (ост. 1)
13) 80140861180306903 / 2 = 40070430590153451 (ост. 1)

14) 40070430590153451 / 2 = 20035215295076725 (ост. 1)
15) 20035215295076725 / 2 = 10017607647538362 (ост. 1)
16) 10017607647538362 / 2 = 5008803823769181 (ост. 0)
17) 5008803823769181 / 2 = 2504401911884590 (ост. 1)
18) 2504401911884590 / 2 = 1252200955942295 (ост. 0)
19) 1252200955942295 / 2 = 626100477971147 (ост. 1)
20) 626100477971147 / 2 = 313050238985573 (ост. 1)
21) 313050238985573 / 2 = 156525119492786 (ост. 1)
22) 156525119492786 / 2 = 78262559746393 (ост. 0)
23) 78262559746393 / 2 = 39131279873196 (ост. 1)
24) 39131279873196 / 2 = 19565639936598 (ост. 0)
25) 19565639936598 / 2 = 9782819968299 (ост. 0)
26) 9782819968299 / 2 = 4891409984149 (ост. 1)
27) 4891409984149 / 2 = 2445704992074 (ост. 1)
28) 2445704992074 / 2 = 1222852496037 (ост. 0)
29) 1222852496037 / 2 = 611426248018 (ост. 1)
30) 611426248018 / 2 = 305713124009 (ост. 0)
31) 305713124009 / 2 = 152856562004 (ост. 1)
32) 152856562004 / 2 = 76428281002 (ост. 0)
33) 76428281002 / 2 = 38214140501 (ост. 0)
34) 38214140501 / 2 = 19107070250 (ост. 1)
35) 19107070250 / 2 = 9553535125 (ост. 0)
36) 9553535125 / 2 = 4776767562 (ост. 1)
37) 4776767562 / 2 = 2388383781 (ост. 0)
38) 2388383781 / 2 = 1194191890 (ост. 1)
39) 1194191890 / 2 = 597095945 (ост. 0)
40) 597095945 / 2 = 298547972 (ост. 1)
41) 298547972 / 2 = 149273986 (ост. 0)
42) 149273986 / 2 = 74636993 (ост. 0)
43) 74636993 / 2 = 37318496 (ост. 1)
44) 37318496 / 2 = 18659248 (ост. 0)
45) 18659248 / 2 = 9329624 (ост. 0)
46) 9329624 / 2 = 4664812 (ост. 0)
47) 4664812 / 2 = 2332406 (ост. 0)
48) 2332406 / 2 = 1166203 (ост. 0)
49) 1166203 / 2 = 583101 (ост. 1)
50) 583101 / 2 = 291550 (ост. 1)
51) 291550 / 2 = 145775 (ост. 0)
52) 145775 / 2 = 72887 (ост. 1)
53) 72887 / 2 = 36443 (ост. 1)
54) 36443 / 2 = 18221 (ост. 1)
55) 18221 / 2 = 9110 (ост. 1)
56) 9110 / 2 = 4555 (ост. 0)
57) 4555 / 2 = 2277 (ост. 1)
58) 2277 / 2 = 1138 (ост. 1)
59) 1138 / 2 = 569 (ост. 0)

60) 569 / 2 = 284 (ост. 1)
61) 284 / 2 = 142 (ост. 0)
62) 142 / 2 = 71 (ост. 0)
63) 71 / 2 = 35 (ост. 1)
64) 35 / 2 = 17 (ост. 1)
65) 17 / 2 = 8 (ост. 1)
66) 8 / 2 = 4 (ост. 0)
67) 4 / 2 = 2 (ост. 0)
68) 2 / 2 = 1 (ост. 0)
69) 1 / 2 = 0 (ост. 1)

$3\text{^}43_{10} = 1000111001011011111011000001001010101001010110010111010111101101111011_2$

Задание 2

$X = 179117333_{10} = 10101010110100011101000101012$

X после циклического сдвига влево на 5: $01011010001110100010101101012$

Задание 3

$2244899301_{10} = 10000101110011100111000111100101_2$

$179117333_{10}\ xor\ 2244899301_{10} =$

$$00001010101011010001110100010101_2$$
$$xor$$
$$10000101110011100111000111100101_2$$
$$=$$
$$10001111011000110110110011110000_2$$

$10001111011000110110110011110000_2 = 2405657840_{10}$

Вывод

Был проведено исследование ассиметричных алгоритмов шифрования, изучено создание ключей в системе PGP, передача подписанных и защищенных сообщений.