КУРСОВА РАБОТА №34

Име: Желязко Ивелинов Георгиев
Факултетен номер: СИ 329
Група: 12

УКАЗАНИЕ Всяка задача изисква съставянето на програма за нейното решаване. Всеки студент самостоятелно защитава своята курсова работа, като представи на електронен носител (или напечатан) кода на програмите и съответните отговори на задачите, които е решавал. *Точки не се присъждат, ако студентът не познава задълбочено кода, който предава.*

Задача 1. (10 точки) Напишете програма, която декриптира шифъра с автоключ, като изчерпва всички възможности за ключа. С нейна помощ дешифрирайте следния текст:

KAPASCEWGGFLTXHSPIVVASNRKGTBDZIRRVXE
DNMPOWAHTHQEWJXMWQMILSPRBYNQPUVQLND
MIFZCYYBVBTSSNVVIDAAJMPIRGBBRGVVBLG
KJEZONARMIURVKKXMBVTINZGWXHHALXKLNA

Задача 2. (15 точки) Напишете програма, която декриптира шифъра с правоъгълник, като изчерпва всички възможности за параметрите m и n. С нейна помощ дешифрирайте следния текст:

SWEOTWIREENUHEVFVLTRRLEIEVWOEVFVNEONE
EOETTFETFUTHXOLTTVERNUVWWEEEIREOONFE
NTOOETOSEWNNLHUIFEEEERRTESIEVIRWLEVN
ENTEEVETOEHLVESWNFRVENEEEOEENFVLNUE

Задача 3. (15 точки) Ще опишем поточен шифър, който използва идея от системата „Енигма“, използвана от Германия през втората световна война. Да предположим, че π е фиксирана пермутация на $\mathbb{Z}_{26}$. Ключът е елемент $K \in \mathbb{Z}_{26}$. За всички цели числа $i \geq 1$, елементът $z_i \in \mathbb{Z}_{26}$ на потока от ключове се дефинира с правилото $z_i = (K + i - 1) \bmod 26$. Криптирането и декриптирането се извършват с помощта на пермутациите π и π^{-1} по следния начин:

$$e_z(x) = \pi(x) + z \bmod 26$$

и

$$d_z(y) = \pi^{-1}(y - z \bmod 26),$$

където $z \in \mathbb{Z}_{26}$. Да предположим, че π е следната пермутация на $\mathbb{Z}_{26}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	9	17	18	8	25	14	13	21	4	16	20	24	10
x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	3	6	2	0	12	5	1	7	15	19	11	23	22

Напишете програма, която декриптира този поточен шифър, като проверява всички възможни ключове. С нейна помощ дешифрирайте следния текст:

XVGQUJDOHWLHJHSWUOPMOZTEXMBXGABYAEBLPIG
RBFQNZXIHQEFRXUEIICNGVKGEGSPNRYWRCPAUV
SUYVFJJDEBDDFROMBUPWRYSQBLPAXJHSRAOPBP
FFOMMKVFJYSTQSEUUDBBYIMMGRKZOKMKVZMOAXV

Задача 4. (20 точки) Напишете програма, която симулира SPN-мрежа. Параметрите са $l = 4$, $m = 8$ и брой рундове $Nr = 20$. Компонентите π_S и π_P на SPN-мрежата са дефинирани по следния начин:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi_S(x)$	6	8	3	1	9	14	0	4	10	13	7	5	12	15	2	11

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(x)$	24	22	29	16	28	1	19	18	7	25	26	31	9	4	11	3
x	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\pi_P(x)$	32	17	13	10	23	15	6	5	27	21	30	2	20	12	8	14

Считаме, че π_S преобразува четворки от битове посредством двоичното представяне на числата от 0 до 15. Ключът на SPN-мрежата е следната последователност от битове:

11001100000011101010000100111010110100110010011101l0

От този ключ получаваме разписанието на подключовете по следния начин: i-тият подключ за $i \in \{1, \ldots, 21\}$ е поднизът на ключа, който започва на позиция i. С помощта на програмата
а) шифрирайте битовата последователност

0000 0001 1110 1011 1100 0010 1111 1110

б) дешифрирайте битовата последователност

1101 1011 1111 0001 0000 1011 1101 0001

Задача 5. (20 точки) Дадена е криптосистема RSA. Параметрите на публичния ключ са $n = 23393$ и $b = 12187$. С помощта на програма разложете n на прости множители и изчислете частния ключ. По-нататък програмата трябва да дешифрира следната последователност от съобщения:

12092 3752 12661 828 5876 2958 17624 20500 2958 8236 20022 18911 2360 868
11732 11891 412 19177 8236 12803 21844 6741 14266 17574 9352 17574 8411
20211 2360 6741 14266 17574 9352 17624 20500 2958 8236 3915 18731 8566
10736 5667 6879 15574 20192 2360 868 12734 6299 16775 13021 10167 18788
18096 2360 8236 17574 12803 21844 12803 21844

Представете отговора като текст на английски, като използвате кодирането на низове с дължина 3 посредством числа.

Задача 6. (30 точки) Дадена е криптосистема на Ел Гамал. Публичният ключ е (p, α, β), където $p = 29683$, α е 10-ият по големина примитивен корен по модул p и $\beta = 15540$. С помощта на програма първо намерете стойността на α и след това стойността на частния ключ. С получените параметри дешифрирайте следната последователност от съобщения:

(23234,18606) (12089,4286) (28242,27890) (9945,17970) (1727,23951)
(10559,7762) (805,25691) (27862,18325) (4695,12512) (12229,13895)
(12946,29020) (3777,6116) (27620,5018) (10389,19448) (15857,14304)
(1126,20170) (2551,26375) (26907,20807) (12021,302) (29321,28583)
(8195,18546) (14709,2582) (12213,17624) (4570,18816) (14732,17535)
(12367,17927) (14675,4587) (2734,26113) (7417,21403) (1431,17314)
(27865,5418) (23964,17061) (11465,17396) (10330,28509) (432,25763)
(19170,5315) (3800,1607) (8117,2869) (28148,27198) (8812,8230) (25652,27569)
(24624,23850) (456,28056) (26253,11316) (23171,18010) (26916,17632)
(16853,25102) (11363,12011) (12253,1048) (4667,18719) (3364,17995)
(26502,12122) (23680,28954) (24569,4596) (27196,26674) (19605,10484)
(15579,5124) (20462,4941) (26721,2938) (19964,7326) (19291,16068)

Представете отговора като текст на английски, като използвате кодирането на низове с дължина 3 посредством числа.