**Група ІПС-41, Шатохін Максим Сергійович**

**Тема: Системи обміну ключами Варіант 16**

**Вхідні дані**

*p* = 5387

*g* = 46

*повідомлення:* you read too loud read much more slowly and with expression

**Завдання**

1. ***Діффі-Хелман.*** Окремо зі своїм абонентом вибрати одному *a* > 100, другому *b* > 100, обчислити окремо ключі *k* і переконатись, що ці ключі співпадають.

2. ***Шамір.*** Перетворити текстове повідомлення у число, закодувавши кожен символ двозначними десятковим числом. Надіслати зашифроване повідомлення своєму абоненту і одержати від нього розшифроване повідомлення.

3. ***Ель-Гамаль.*** Обмінятися ключами.

Описати хід виконання завдання.

Робота виконана разом зі студентом Бухало Михйлом Олександровичем Групи ІПС-41 варіант 1, який надалі буде позначатися, як *студент* , а я, Шатохін Максим буду зазначений як *студент* .

**Розв’язання**

***Завдання №1***

***Перший випадок:***

Взяті числа , з 1го варіанту.

Генерую елемент: .

Обчислюю число: , та надсилаю його студенту .

Отримую відкритий ключ від студента .

Обчислюю спільний ключ: – має співпадати з спільним ключем студента .

***Другий випадок:***

Отримую числа , та відкритий ключ від студента .

Генерую елемент: .

Обчислюю число: , та надсилаю його студенту .

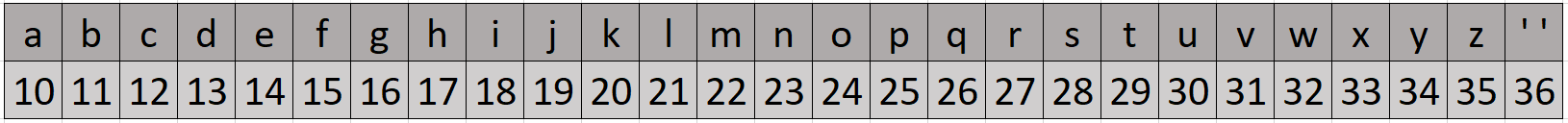
Обчислюю спільний ключ: – має співпадати з спільним ключем студента .

***Завдання №2***

***Перший випадок:***

Взято число та повідомлення *t = “* you read too loud read much more slowly and with expression *”* з 16-го варіанту.

Нумеруємо символи як в таблиці (включно з пробілом):



Кожний символ повідомлення *t* переводжу в числове значення згідно з таблицею:

*m=* *3424303627141013362924243621243013362714101336223012173622242714362821243221343610231336321829173614332527142828182423*

Розбиваю число на блоки чисел менші за :

*m= [3424, 3036, 2714, 1013, 3629, 2424, 3621, 2430, 1336, 2714, 1013, 3622, 3012, 1736, 2224, 2714, 3628, 2124, 3221, 3436, 1023, 1336, 3218, 2917, 3614, 3325, 2714, 2828, 1824, 23]*

Для кожного числа з знаходимо та , такі що та :

*[()] = [(4749, 2173), (1511, 5165), (3395, 1569), (3715, 361), (2109, 4081), (4227, 79), (1397, 2853), (3185, 2797), (4421, 2573), (3559, 737), (4277, 4031), (1499, 4247), (1641, 4467), (2441, 1977), (5033, 3433), (2289, 2673), (3449, 4727), (4129, 4709), (4051, 5269), (2069, 2611), (1439, 5255), (2213, 3125), (1071, 1911), (4929, 5221), (2525, 1619), (3009, 4423), (851, 981), (2511, 873), (2781, 5233), (883, 3611)]*

Шифруємо кожне за формулою :

*= [59, 4878, 1666, 5082, 4579, 2005, 4959, 3774, 3557, 335, 2193, 4631, 2618, 4578, 1118, 2912, 5379, 4999, 2338, 2082, 3828, 1254, 1647, 1083, 410, 1643, 3345, 4851, 2039, 1495]*

Надсилаємо число , та таблицю відповідності символів до числа студенту .

Від студента отримуємо , яке дорівнює:

*= [2921, 584, 2770, 727, 3918, 582, 3731, 5385, 2726, 4852, 804, 2811, 3424, 4089, 3397, 5197, 2682, 4767, 1960, 3543, 581, 1026, 3603, 671, 1570, 1508, 1126, 602, 4634, 4358]*

Обчислюємо :

*= [1052, 4575, 5039, 4330, 3091, 4075, 2575, 3379, 3984, 4562, 4761, 406, 5212, 5139, 3121, 1034, 715, 3786, 5201, 698, 4616, 785, 4349, 3891, 4189, 3674, 1398, 1039, 2460, 981]*

Надсилаємо число студенту , після розшифрування він повинен буде отримати вхідне повідомлення *t = “* *you read too loud read much more slowly and with expression”*.

***Другий випадок:***

Від студента отримую число , таблицю відповідності символів до чисел, яка співпадає з першим випадком та число рівне:

*= [2777, 2318, 3472, 351, 1711, 566, 2039, 277, 1859, 3915, 2236, 2927, 1073, 1341, 1193, 417, 1302, 2196, 718, 1225, 2735, 2234, 2817, 1255, 2110, 791, 845, 2191, 152, 1542, 3280]*

Для кожного числа з знаходимо та , такі що та :

*[()] =[* *(1469, 1147), (3887, 2809), (913, 255), (3417, 1835), (1831, 1709), (27, 2923), (2627, 3587), (377, 3789), (3885, 1035), (257, 737), (2953, 3187), (1559, 1139), (1177, 2263), (253, 2979), (2459, 2245), (3851, 1703), (2957, 3551), (2069, 1377), (3111, 2533), (3181, 1011), (3325, 1417), (2039, 2541), (3303, 583), (1109, 3793), (3257, 3883), (2589, 3725), (1933, 1825), (1185, 1645), (989, 395), (803, 3317), (2071, 2275)]*

Шифруємо кожне за формулою :

*= [48, 2848, 3182, 2968, 697, 1093, 1699, 3817, 24, 524, 3244, 1551, 3834, 1829, 1595, 330, 107, 1944, 1640, 3705, 3629, 690, 2115, 273, 962, 1515, 2603, 1320, 3745, 3200, 2430]*

Надсилаємо число студенту .

Від студента отримуємо , яке дорівнює:

*= [3158, 1636, 1496, 3170, 1181, 1594, 1454, 674, 17, 495, 3787, 208, 891, 148, 1905, 2338, 1389, 2554, 3036, 1989, 2142, 2753, 1671, 1152, 1821, 381, 2540, 724, 3075, 3593, 3534]*

Обчислюємо :

*= [1823, 3629, 1718, 2836, 2114, 1229, 3027, 1436, 1836, 1022, 3616, 2418, 2316, 3629, 2436, 1013, 1327, 1428, 2836, 2917, 1436, 1524, 2121, 2432, 1823, 1636, 2630, 1428, 2918, 2423, 28]*

Об’єднуємо у одне число :

*m=* *18233629171828362114122930271436183610223616241823163629243610131327142828362917143615242121243218231636263014282918242328*

Переводимо з кожні дві цифри за допомогою таблиці відповідності у символ, отримуємо повідомлення з 1-го варіанту: *t = “* *in this lecture i am going to address the following questions ”*.

***Завдання №3***

***Перший випадок:***

Отримую числа , від студента .

Взято повідомлення з 16го варіанту: *t = “*you read too loud read much more slowly and with expression*”*.

За допомогою таблиці з ***завдання №2***, переводжу повідомлення в число:

m= 3424303627141013362924243621243013362714101336223012173622242714362821243221343610231336321829173614332527142828182423

Розбиваю число на блоки чисел менші за :

*m= [3424, 3036, 2714, 1013, 3629, 2424, 3621, 2430, 1336, 2714, 1013, 3622, 3012, 1736, 2224, 2714, 3628, 2124, 3221, 3436, 1023, 1336, 3218, 2917, 3614, 3325, 2714, 2828, 1824, 23]*

Запитую публічних ключів від студента для того, щоб зашифрувати повідомлення:

*=* *[3598, 142, 1622, 218, 241, 732, 673, 1125, 149, 2288, 2929, 3743, 1978, 3723, 1295, 1714, 3130, 1604, 2870, 1663, 2714, 2813, 2303, 3224, 1320, 200, 2200, 3225, 1140, 567]*

Шифруємо кожне за формулою обираючи кожного разу випадкове , яке належить проміжку , отримуємо пари чисел:

*[] =[* *(3809, 2646), (1369, 2628), (3267, 207), (2990, 832), (2170, 1724), (612, 2673), (2820, 1958), (3150, 3372), (644, 2861), (2772, 688), (554, 298), (1607, 65), (2877, 1655), (696, 2702), (2272, 797), (2423, 3383), (297, 2182), (1503, 3859), (1379, 1372), (1459, 78), (1428, 3649), (3210, 2208), (3916, 2535), (2973, 2762), (3319, 1194), (242, 2682), (3713, 462), (951, 2195), (2277, 1217), (2827, 2472)]*

Надсилаємо пари чисел студенту , після розшифрування він повинен буде отримати вхідне повідомлення *t = “you read too loud read much more slowly and with expression”*.

***Другий випадок:***

Взяті числа , з 16го варіанту.

Надсилаю числа та студенту .

Отримую від студента , кількість ключів потрібних для шифрування .

Генерую випадкові приватних ключі , де :

*c = [5316, 2189, 3823, 4378, 612, 1474, 591, 2216, 3938, 782, 628, 1094, 189, 1268, 936, 1427, 2814, 3016, 4946, 1046, 3677, 279, 2355, 552, 3032, 491, 3137, 940, 3166, 4319, 498]*

Для кожного приватного ключа генерується публічний ключ за формулою :

*d = [2564, 873, 3831, 2562, 5291, 3483, 4792, 2357, 1030, 5105, 3356, 2983, 4287, 3759, 4576, 1219, 5385, 5349, 791, 356, 5358, 1082, 879, 1974, 3573, 5339, 5311, 3661, 2335, 2165, 144]*

Надсилаю публічні ключі студенту .

Отримую від студента зашифроване повідомлення у вигляді пар чисел :

*[]=[* *(2519, 3545), (2347, 554), (134, 4995), (5185, 4563), (718, 565), (4630, 5263), (4544, 4669), (2647, 3052), (1469, 4359), (1167, 5022), (1720, 527), (4995, 4083), (5031, 5040), (3354, 4848), (4107, 1894), (984, 537), (4227, 630), (1890, 5154), (1488, 3164), (4179, 5168), (4665, 536), (5169, 5017), (2758, 1679), (4005, 3760), (3973, 2746), (4875, 1108), (899, 2259), (1372, 1067), (5307, 3355), (1709, 4873), (2230, 1053)]*

Розшифруємо кожне за формулою :

*m=[1823, 3629, 1718, 2836, 2114, 1229, 3027, 1436, 1836, 1022, 3616, 2418, 2316, 3629, 2436, 1013, 1327, 1428, 2836, 2917, 1436, 1524, 2121, 2432, 1823, 1636, 2630, 1428, 2918, 2423, 28]*

Об’єднуємо у одне число:

*m=* *18233629171828362114122930271436183610223616241823163629243610131327142828362917143615242121243218231636263014282918242328*

Переводимо з кожні дві цифри за допомогою таблиці відповідності у символ, отримуємо повідомлення з 16-го варіанту: *t = “in this lecture i am going to address the following questions”*.