**Група ІПС-42, Гончарук Ангеліна Віталіївна**

**Тема: Системи обміну ключами Варіант 25**

**Вхідні дані**

*p* = 6047

*g* = 55

*повідомлення:* the conference will be chaired by mister nnn

**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.

**Варіант партнера 27**

**1. Діффі-Хелман**

**ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ ДІФФІ-ХЕЛМАНА**

**Вхід:** пара *(р, д),* де *р* - велике просте число, а *g* - породжуючий елемент групи поля *Fp* (1 < *g < р* — 1);.

**Вихід:** елемент групи *k,* яким необхідно обмінятися абонентам *А* і *В.*

1. *А* генерує елемент *а* Є [1,р — 1), обчислює число *gа = gа (mod p)* і висилає його абоненту *В.*

2. *В* генерує елемент *Ь* Є [1,р — 1), обчислює число *gb = gb (mod р)* і висилає його абоненту *А.*

3. *А* обчислює число *k = gab (mod р).*

*4. В* обчислює число *k = gba (mod р).*

Умовою задані g=55 та p=6047.

Мною генерується a = 5376.

g = 555376 mod 6047 = 5404

Надсилаю 5404.

Отримую 2823.

Обчислюю k = 54042405 mod 6047= 4677.

Отримую 4677.

Отримані числа однакові.

Тепер повторюємо те ж саме для p = 6659 та g = 57з варіанта 27 Гринь.

Генерую b = 1130 та g= 57 1130 mod 6659 = 3920. Надсилаю 3920 Гринь.

Отримую 1736. Обчислюю k= 3920 6303 mod 6659 = 4636. Отримую 4636.

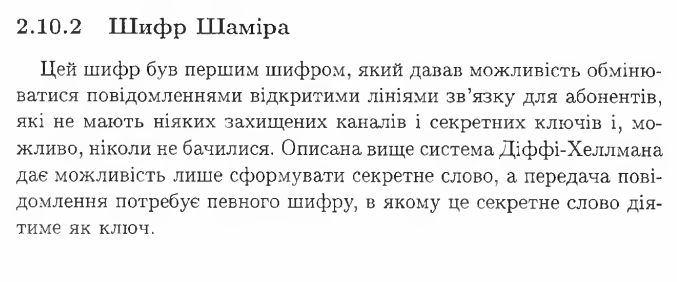
Отримані числа однакові.

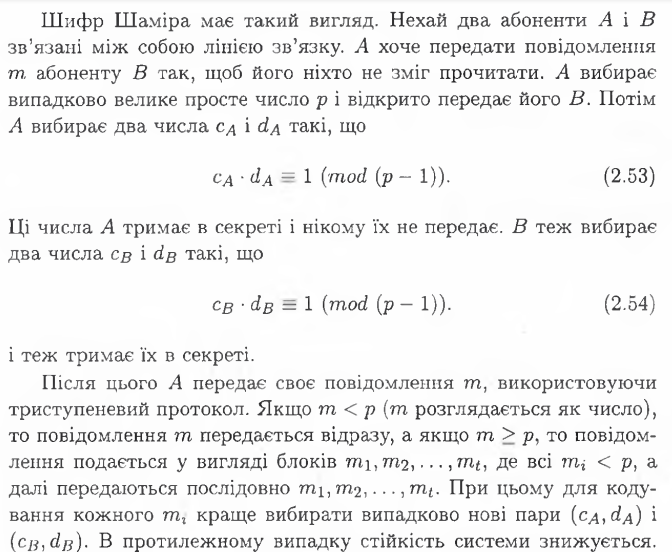
**2. Шамір**

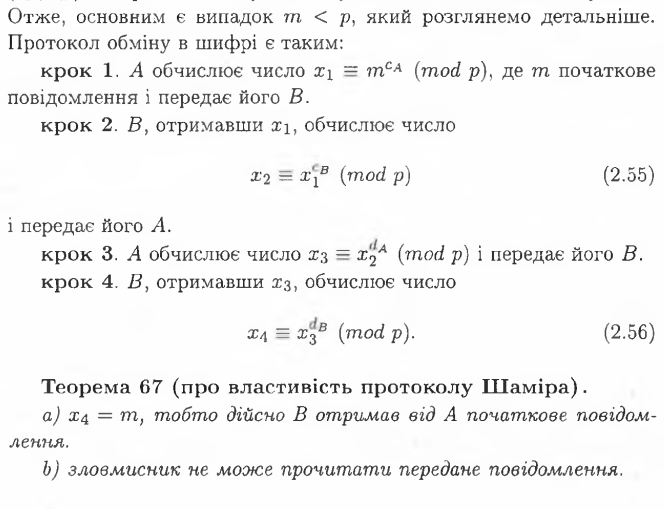
Кодуємо символи повідомлення:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| t | h | e |  | c | o | n | f | e | r | e | n | c | e |  | w | i | l | l |  | b | e |  |
| 41 | 44 | 32 | 90 | 13 | 18 | 19 | 51 | 32 | 55 | 32 | 19 | 13 | 32 | 90 | 60 | 2 | 66 | 66 | 90 | 71 | 32 | 90 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| c | h | a | i | r | e | d |  | b | y |  | m | i | s | t | e | r |  | n | n | n |
| 13 | 44 | 3 | 2 | 55 | 32 | 39 | 90 | 71 | 85 | 90 | 7 | 2 | 79 | 41 | 32 | 55 | 90 | 19 | 19 | 19 |







Закодовуємо моє повідомлення щоб передати партнеру:

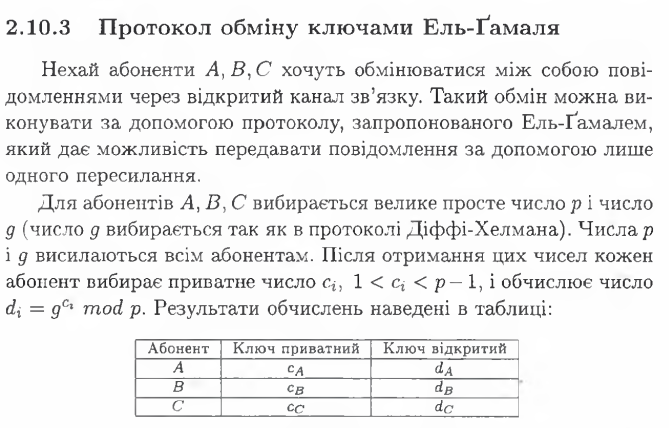
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Моє повідомлення** | **Ca** | **Da** | **Крок 1** | **Крок 3** |
| t | 827 | 4211 | 715 | 3453 |
| h | 2987 | 2939 | 1149 | 6034 |
| e | 1613 | 551 | 1032 | 1921 |
|  | 2019 | 4947 | 3816 | 790 |
| c | 1157 | 3799 | 4914 | 5139 |
| o | 591 | 2445 | 1459 | 5501 |
| n | 3579 | 2289 | 2299 | 4218 |
| f | 807 | 5117 | 2392 | 5854 |
| e | 2085 | 1215 | 1830 | 2667 |
| r | 4927 | 4625 | 953 | 5655 |
| e | 3815 | 5775 | 891 | 5438 |
| n | 2457 | 1629 | 1973 | 5059 |
| c | 3063 | 5517 | 1562 | 1566 |
| e | 4129 | 41 | 355 | 5235 |
|  | 2751 | 3901 | 3623 | 4111 |
| w | 2855 | 3005 | 4275 | 430 |
| i | 3013 | 5139 | 5486 | 3612 |
| l | 3035 | 3275 | 2 | 3370 |
| l | 3395 | 2251 | 444 | 1169 |
|  | 4081 | 3003 | 5619 | 5089 |
| b | 1765 | 2069 | 1197 | 5935 |
| e | 2825 | 4107 | 876 | 2510 |
|  | 1667 | 5803 | 4176 | 4425 |
| c | 3467 | 2703 | 3129 | 4371 |
| h | 4293 | 1959 | 498 | 1060 |
| a | 1377 | 2551 | 5350 | 4758 |
| i | 1023 | 1643 | 5055 | 5614 |
| r | 3967 | 823 | 2438 | 3654 |
| e | 3467 | 2703 | 5721 | 4541 |
| d | 3555 | 483 | 5917 | 2532 |
|  | 2533 | 4917 | 5655 | 3816 |
| b | 5483 | 1933 | 1562 | 2696 |
| y | 89 | 1019 | 1590 | 4036 |
|  | 3713 | 977 | 405 | 5765 |
| m | 2953 | 4189 | 4 | 167 |
| i | 3145 | 5823 | 2241 | 878 |
| s | 3479 | 2075 | 1161 | 700 |
| t | 773 | 5827 | 3936 | 5503 |
| e | 1471 | 933 | 5029 | 5072 |
| r | 4261 | 105 | 1475 | 4618 |
|  | 3113 | 5475 | 995 | 5413 |
| n | 3883 | 3139 | 1919 | 4420 |
| n | 5965 | 5001 | 2712 | 2051 |
| n | 1449 | 1185 | 2953 | 393 |

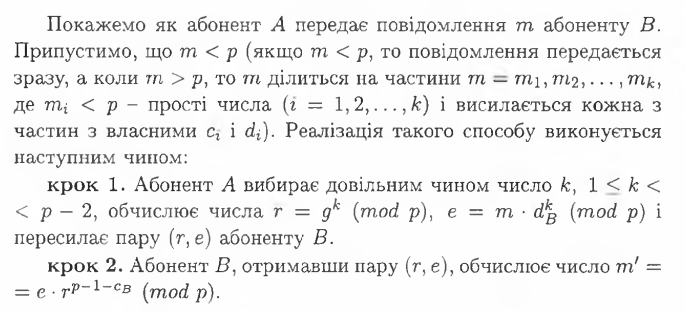
Розкодовуємо отримане повідомлення:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Cb | Db | Крок 2 | Крок 4 | Отримане | Кінцеве |
| 1779 | 1759 | 2840 | 98 | 2 | i |
| 1415 | 5237 | 3723 | 4116 | 90 |  |
| 2951 | 5381 | 3578 | 2384 | 3 | a |
| 4029 | 623 | 2598 | 2546 | 7 | m |
| 4155 | 133 | 871 | 4922 | 90 |  |
| 355 | 4745 | 447 | 1595 | 13 | c |
| 5955 | 2273 | 4473 | 3183 | 18 | o |
| 3103 | 2401 | 715 | 6620 | 19 | n |
| 5231 | 1661 | 6549 | 5729 | 26 | v |
| 4039 | 4037 | 2044 | 2562 | 2 | i |
| 4449 | 5799 | 4031 | 2342 | 19 | n |
| 6625 | 807 | 6192 | 5050 | 13 | c |
| 4231 | 1229 | 511 | 5218 | 32 | e |
| 6083 | 3439 | 709 | 15 | 39 | d |
| 3031 | 2089 | 1395 | 3949 | 90 |  |
| 2865 | 2877 | 5790 | 5009 | 41 | t |
| 53 | 1005 | 919 | 4287 | 44 | h |
| 3015 | 2237 | 3294 | 3035 | 3 | a |
| 2101 | 5739 | 2815 | 1107 | 41 | t |
| 4025 | 1411 | 888 | 2447 | 90 |  |
| 2313 | 3175 | 3872 | 1497 | 41 | t |
| 5267 | 4887 | 394 | 4408 | 44 | h |
| 3319 | 6325 | 2346 | 3337 | 32 | e |
| 5883 | 189 | 5252 | 3877 | 90 |  |
| 907 | 2995 | 5641 | 2898 | 41 | t |
| 4537 | 1783 | 3723 | 3871 | 18 | o |
| 3317 | 1387 | 527 | 1629 | 49 | p |
| 4323 | 5737 | 4856 | 2778 | 2 | i |
| 5861 | 6115 | 1683 | 601 | 13 | c |
| 1793 | 557 | 2014 | 2109 | 90 |  |
| 1783 | 4537 | 1349 | 5698 | 18 | o |
| 6613 | 3255 | 6435 | 438 | 51 | f |
| 3271 | 6371 | 4762 | 2175 | 90 |  |
| 2073 | 6385 | 5570 | 3627 | 41 | t |
| 4751 | 5649 | 6523 | 3988 | 44 | h |
| 6435 | 6449 | 3077 | 5991 | 32 | e |
| 1135 | 6001 | 5813 | 4933 | 90 |  |
| 5467 | 1951 | 328 | 792 | 13 | c |
| 3061 | 5627 | 4898 | 2943 | 18 | o |
| 4367 | 1889 | 5652 | 1639 | 19 | n |
| 4159 | 1849 | 4083 | 6440 | 51 | f |
| 3307 | 2875 | 4917 | 2619 | 32 | e |
| 4559 | 1789 | 2738 | 2914 | 55 | r |
| 6325 | 3319 | 1060 | 4275 | 32 | e |
| 6629 | 2755 | 797 | 63 | 19 | n |
| 603 | 4527 | 267 | 4334 | 13 | c |
| 3455 | 3831 | 19 | 2053 | 32 | e |
| 5897 | 4427 | 4703 | 434 | 90 |  |
| 1501 | 621 | 1317 | 2850 | 60 | w |
| 1401 | 1535 | 2800 | 4816 | 2 | i |
| 6197 | 4145 | 3406 | 3447 | 66 | l |
| 5429 | 2427 | 5426 | 1787 | 66 | l |
| 2301 | 2011 | 1491 | 5254 | 90 |  |
| 5597 | 2987 | 1932 | 3805 | 71 | b |
| 3041 | 1861 | 781 | 689 | 32 | e |
| 507 | 2981 | 6599 | 418 | 90 |  |
| 2249 | 4713 | 5218 | 4649 | 18 | o |
| 4139 | 3703 | 3282 | 3166 | 51 | f |
| 3989 | 459 | 212 | 5206 | 90 |  |
| 3271 | 6371 | 5766 | 2485 | 78 | g |
| 4781 | 3235 | 1763 | 6620 | 55 | r |
| 2067 | 4123 | 1520 | 4395 | 32 | e |
| 1675 | 2695 | 5022 | 5082 | 3 | a |
| 5265 | 4923 | 6622 | 1386 | 41 | t |
| 2161 | 2511 | 3508 | 6207 | 90 |  |
| 2581 | 6253 | 4568 | 6070 | 2 | i |
| 5351 | 6225 | 1801 | 1679 | 19 | n |
| 6423 | 6573 | 2355 | 4777 | 41 | t |
| 2377 | 2773 | 6303 | 159 | 32 | e |
| 5627 | 3061 | 5170 | 4787 | 55 | r |
| 1523 | 4223 | 1338 | 3491 | 32 | e |
| 4623 | 301 | 1058 | 3041 | 79 | s |
| 5689 | 213 | 2552 | 4043 | 41 | t |

**Результат:** i am convinced that the topic of the conference will be of great interest

**3. Ель-Гамаль.**





Кодування літер беремо із завдання 2.

m = 41, с1 – беремо випадкове число від 1 до p-2.

p i g – беремо з умови задачі (вони відомі всім учасникам).

*p* = 6047

*g* = 55

d1 = gc1 mod p = 551787 mod 6047 = 1208

k – випадкове число



r = 55963 mod 6047 = 1724

e = 41 \* 1208963 mod 6047 = 3621

Інші длітери кодуються аналогічно.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***m*** | ***c1*** | ***d1*** | ***k*** | ***r*** | ***e*** |
| 41 | 1787 | 1208 | 963 | 1724 | 3621 |
| 44 | 3953 | 3319 | 6481 | 6521 | 560 |
| 32 | 1407 | 6152 | 1289 | 4170 | 2271 |
| 90 | 6167 | 6444 | 471 | 4946 | 4056 |
| 13 | 4777 | 966 | 3264 | 3469 | 2236 |
| 18 | 5984 | 960 | 2676 | 558 | 902 |
| 19 | 4191 | 1921 | 5571 | 360 | 5903 |
| 51 | 4067 | 2103 | 212 | 1473 | 4377 |
| 32 | 1125 | 712 | 3911 | 6457 | 4268 |
| 55 | 3155 | 6051 | 3594 | 400 | 1571 |
| 32 | 2330 | 5115 | 4514 | 2575 | 2286 |
| 19 | 5553 | 2598 | 3552 | 3573 | 4551 |
| 13 | 5419 | 6542 | 5406 | 1524 | 215 |
| 32 | 2452 | 5057 | 3581 | 1278 | 2043 |
| 90 | 1642 | 119 | 2979 | 1366 | 3871 |
| 60 | 1946 | 4003 | 2065 | 3067 | 6170 |
| 2 | 3220 | 5828 | 4254 | 3266 | 2331 |
| 66 | 4926 | 432 | 2404 | 3513 | 744 |
| 66 | 5198 | 1985 | 3036 | 114 | 2970 |
| 90 | 970 | 6418 | 671 | 4545 | 5291 |
| 71 | 2444 | 5781 | 575 | 6485 | 5817 |
| 32 | 6045 | 674 | 4048 | 5132 | 5932 |
| 90 | 2514 | 3895 | 1462 | 1055 | 6006 |
| 13 | 6389 | 1561 | 1706 | 3341 | 516 |
| 44 | 1961 | 4821 | 2897 | 4459 | 6205 |
| 3 | 4848 | 5362 | 3464 | 6388 | 3266 |
| 2 | 714 | 1813 | 2262 | 617 | 4802 |
| 55 | 6546 | 359 | 1109 | 2779 | 6622 |
| 32 | 451 | 4302 | 2036 | 3088 | 3924 |
| 39 | 6522 | 1983 | 745 | 4508 | 525 |
| 90 | 2372 | 3480 | 1883 | 6104 | 6044 |
| 71 | 1421 | 2022 | 4507 | 4375 | 3201 |
| 85 | 3974 | 1109 | 126 | 593 | 5324 |
| 90 | 4462 | 961 | 2169 | 813 | 1383 |
| 7 | 452 | 5490 | 6356 | 930 | 6520 |
| 2 | 1168 | 4549 | 5439 | 367 | 981 |
| 79 | 1957 | 1845 | 6026 | 907 | 5905 |
| 41 | 6543 | 5548 | 6160 | 5130 | 171 |
| 32 | 2799 | 5899 | 111 | 2480 | 2753 |
| 55 | 3919 | 4182 | 774 | 4900 | 6098 |
| 90 | 3241 | 3105 | 2771 | 4095 | 6302 |
| 19 | 6473 | 4239 | 2302 | 5866 | 5818 |
| 19 | 4682 | 2283 | 1915 | 1248 | 5785 |
| 19 | 4042 | 4758 | 5967 | 2015 | 5823 |

Передаємо r i e партнеру.