Задание на лабораторную работу

Реализовать на языке Python 3.7.6 процедуры, составляющих протокол доказательства с нулевым разглашением секрета.

Основные теоретические положения

Идея протоколов доказательства с нулевым разглашением секрета заключается в том, что один пользователь (доказывающий) может убедить другого (проверяющего) в том, что он владеет некоторым секретом, без раскрытия самого секрета.

Многораундовые протоколы с нулевым разглашением включают многократное повторения трех типовых шагов:

1. генерация доказывающим разового случайного секретного ключа и вычисление по нему разового открытого ключа, который передается (объявляется) проверяющему и часто называется фиксатором;
2. генерация проверяющим нулевого ($r = 0$) или единичного ($r = 1$) запроса с вероятностью 0,5 и направление бита запроса r доказывающему;
3. вычисление доказывающим ответа w и передача w проверяющему.

После каждого такого трехшагового раунда проверяющий подставляет полученный им ответ в некоторое проверочное соотношения, в которое входят значения фиксатора, открытого ключа и запроса r. Если это соотношение выполняется то, проверяющий считает, что текущий ответ правильный.

Протокол Фиата-Шамира.

Протокол основан на сложности извлечения квадратного корня по составному модулю, включающему не менее двух больших простых множителей.

1. Доказывающий выбирает два больших простых числа p и q и вычисляет модуль $n := pq$;
2. Выбирает случайное число s (личный секретный ключ), такое, что $1 \leq s \leq n - 1$;

3. Вычисляет значение открытого ключа $y := s^2 \, mod \, n$;

4. Повторение z -раз раунда:

4.1 Доказывающий выбирает случайное число k, такое, что $1 \leq k \leq n - 1$,

вычисляет значение фиксатора $u := k^2 \, mod \, n$,

посылает фиксатор проверяющему.

4.2 Проверяющий отправляет доказывающему равновероятный случайный бит r.

4.3 Доказывающий вычисляет значение $w := ks^r \, mod \, n$ и отправляет его.

5. Проверяющий считает ответ верным, если выполняется соотношение $w^2 = uy^r \, mod \, n$.

Действия нарушителя.

Возможны два развития событий после выбора злоумышленником случайного числа k:

1. Расчет фиксатора по формуле $u := k^2 \, mod \, n$ приведет к тому, правильный ответ может быть получен только в случае $r = 0$.
2. Расчет фиксатора по формуле $u' := \frac{k^2}{y} \, mod \, n$ приведет к тому, правильный ответ может быть получен только в случае $r = 1$.

Таким образом, нарушитель в лучшем случае может правильно ответить только на один вопрос, и в одном раунде с вероятностью 1/2 попытка обмана обнаруживается.

Нулевое раскрытие.

По запросу проверяющего $r = 0$ доказывающий направляет ему случайное число k, но проверяющий самостоятельно мог бы сгенерировать случайное число k', возвести его в квадрат, получив значение $u' := k'^2 mod \, n$.

По запросу проверяющего $r = 1$ доказывающий направляет ему случайное число w, но проверяющий самостоятельно мог бы сгенерировать случайное число w' и вычислить случайное значение $u' := \frac{w'^2}{y} \ mod \ n$.

Проверяющий при получении пары случайных чисел (u, w), связанных соотношением $w^2 = uy \, mod \, n$, сможет вычислить квадратный корень из случайного числа u, затем он легко вычислит секретное значение s.

Таким образом, данные, полученные в процессе выполнения описанного протокола проверяющим от доказывающего, не дают никаких новых возможностей проверяющему для вычисления секретного ключа.

Разработка программы

Программа разрабатывалась для операционной системы Windows. Для создания программы, реализующую функционал подписи, был выбран язык Python 3.

В реализации алгоритма используются функции:

- `range([start=0], stop, [step=1])` - арифметическая прогрессия от `start` до `stop` с шагом `step`;

- `random.randint(A,B)` - случайное целое число `N, A ≤ N ≤ B`.

- `count(x)` - возвращает количество элементов со значением `x;`

- `append(x)` – добавляет элемент `x` в конец списка;

- `format(u, 'x')` – преобразование числа `u` в строку в 16-тиричном виде.

Повторение раундов реализовано с помощью цикла for. В начале каждого раунда случайно выбирается число k, и идет расчет фиксатора. Случайно выбирается бит, рассчитывается w и делается проверка. Результат проверки (0 или 1) записывается в список результатов.

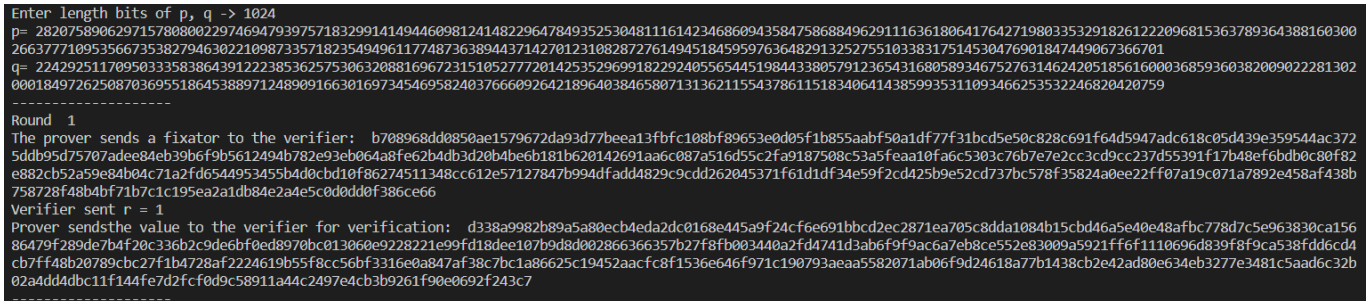
```
for i in range(1, z + 1):
    print('--------------------')
    print('Раунд ', i)
    # доказывающий:
    k = random.randint(1, n - 1)
    u = (k**2) % n
    print('Доказывающий отправляет проверяющему фиксотор: ', format(u, 'x'))
    # проверяющий:
    r = random.randint(0, 1)
    print('Проверяющий отправил r =', r)
    # доказывающий:
    w = (k * (s**r)) % n
    k = 0
```

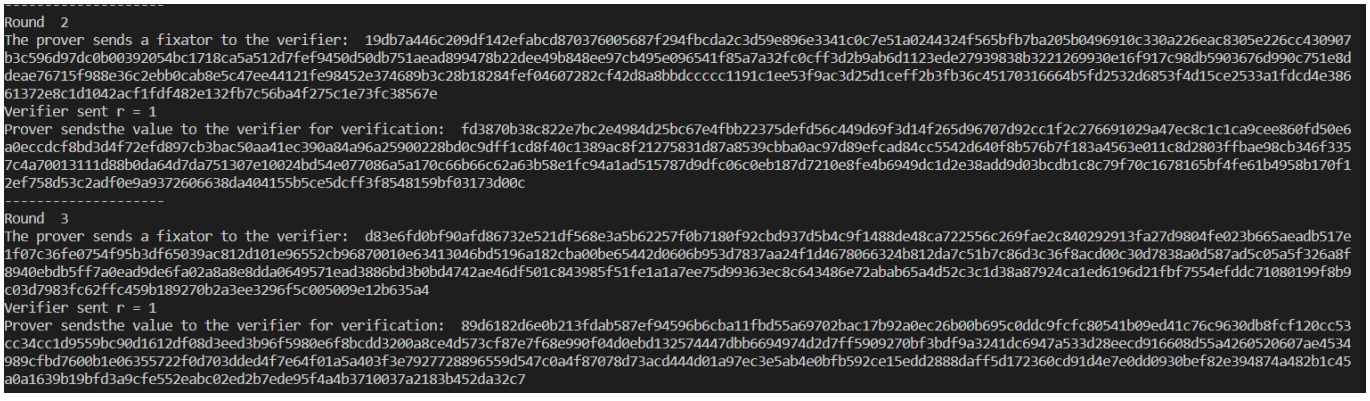
```
            print('Доказывающий отправляет'
                  'проверяющему значение на проверку: ',
format(w, 'x'))
            # проверяющий
            if ((w**2) % n == (u * y**r) % n):
                res.append(1)
            else:
                res.append(0)
```

По завершении всех раундов просматриваются результаты и выводится соответствующее сообщение:

```
    if res.count(0) != 0:
        print('Проверка не пройдена')
    else:
        print('Проверка пройдена')
```

Screenshots:





```
--------------------
Round  4
The prover sends a fixator to the verifier:  8f7f068c74b0ad12f35713d75154038a63c0d03a0487a0dd6d2c4c7d74b4f47a74d028df405340611bbe760c2b90ec1261009e06dda6fdffa268beacdda
7f7ed336fcdd5c1b65b02520d2d5a65083cd4f6016f572fe7d50d2ba36c8dc5118d47cbda8487a0266a82a85a2e89256ef3905c35945d71e54a88cdf3deecbabdd6b66e4009fedde4d9efd35e646fa43c1a64127
1ff32f5a25d9330ad7576b5d206441e82e4e25c47ad0b9c1888f1b8e563826202b70140c0abae23ac3168bc20bf5eb2d2d8ae97dfa099fb9fd07e8559cedbeb1ef8bcff1cd861a2d29619554052d51751a44008e
841c6113c3e63352cc1d9e23223d1d35037bfdd2e580d7126ee19
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  197c1783d53370bb3325efb24007b0bdc026cbe532fd91de0b8d52714103511f4fb952c867661f3ad1fd2a531ab0cbcccf46f3af8a2d68d
de757d8cfeda525c46289d28a51bf9df11f2e0117120324eb4d35c56a188cb1dd10aa99f6e38aedca7ed08f4067be0d2e30cd2242233eb891b9ebffaee822a8dce00dce477ffa3552192ba51f381133a40ea5d26
1df2db71244a4ef9e5daadd6d0e4ae2fdd703ef6b80ebebb0d373244b488121db458e4a036c9f18a5b5d35be10632650a08af68439785c767b3cfb99399235e895f8370bb333b29398e4274934be106d25d2ac4b
c514c9478cbde2d07551220046520cac95e58ff7535abdf4dffca3956770e9a0bd
--------------------
Round  5
The prover sends a fixator to the verifier:  d62b0210887985a3af1fe4c08243f2451dd42207167e36cb292f2a0a875ea3cb9c2d400baf7540e7b4c523bfc774b7c4704527db417ae0307ac6e75bd14
ff702857cf889170555496a25e39f2e88ec3631d90018156fa80c02fc8ba400cffa11260957e2300ea999ac2d549ced1a4c31f16969dac4aa9bd1bb9247bd8795f3ff9e34fd002859735c6eddee02bc0b120b628
bf415c12d00b2c3d1993a190cc5eb64f32c1b07f04e9bef1fcae2a474d5a62d71f140117a090ea1c1997a4d617fa2a6ba949e24fb80a923182ca6a200199cfede729cce6d5d34e3cd4f9b3eb332935bf445c176b
50c1722fce9ef659a414849f588ac994510bfba236a5f2460faed
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  16d575ecb14cc0694f147972405529e63976dc0c9e84e19ed94ad6bcab721439c745c356196205946fbda3184c89be92b7d221cfbb9f187
1d0fb173e34cc4d5e3726829d39ff9f30099b5290fba0061b409bd376c81e52781ead4167f1c82c57a3a9a02582f9a098fc92d0eee90c4c0deb42e341049f69043342e4f7fa5003a4fc9206584d51556e0a9d594
59f4f849373770d7032d56af7d1d8aebe4e13449503cd47d0c7d7ef0c7d91f6937322b6aa95ff6d7cfa4770d96c021fcc0b16fc27a832dd974096c04a89370de5f394e99b57342fb249095501508680cedac0209
1e155497f2c3fab203ab20f9d0e4ba0f41c5062cce1d4dcc93bb3a202bb6b61db8
```

```
--------------------
Round  6
The prover sends a fixator to the verifier:  277b0ca69266245d4f93199c2be0bd6cbeaabfe1df81b4171873cd23fdb031a1b1ad7c33da0a632da9c5f043f892441cad11637461e5f2df65bc8905887
e4736500bf4d8ead656bfbf40ef7815665b502d8214490bfc6ef16a0c1cc12efab7917c04b6c3877ed6a70f67f895c8c2c108ff7090b95b100b0dc2ac137243feba3cd5d3d6cde160ac433f55ae2fa86f3416e39
c35b28961320aa0195d1f7aff97aeb1030e07249b7edad2a380af9dfef5aa535c2506f522ab2b85b7caeb8fdb8862d14c99fa203b9c10d3b5928f9e530f34f40a38b818db6fc9f0c28140914726ed307b0dc257a
93671dcebf9908499e9b5ae86f4dce585c00fc0fe9cfa89f67e26
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  aed885b1baf08a82858315e881290e81d2d5ea070b97c4f0700b3c0abb4163cfbb5535f74f03c3a15672646eaf296b71399df2d9d1d594a
0439a9981f248db04c21a8117c5ccf4fa6ee098c120a05e5ea203d78e86a457a5504fbb02a2e2d353ce36a01e6ccd62ea33ebcd7c1ae322177ff1098d4f5865ee0049b694facb9aead5c6466fd1633dbe24776f7
071509e42a217b49e30e796c2e5f594ee57eb4d668a5ec37f46e111e09fb4d9ee21f9e09b71ec18d1e288f7f959b253bfdc21c0c9741d633dd673c91e58eb42741ec716f071d3674b3c843133d2199d88e6a7029
e8baf5e7df1f00fe1afa632488ea5a55931fb12976d06b78db3cbeb7eec96aa1
--------------------
Round  7
The prover sends a fixator to the verifier:  1c7f8cea0b8c4c331f6825e2d4ac8e736b667e305467a46c80a7cfe4ea29bd23b3b241bda178b8fa4528db7a50d665c22b87a9ab227cd77aed3589e4bf9
62ca8624bde6e9be762926cfbc68a95376f7989a19f22ba8302de0df4f5d76bcf1b2d743168b3f1b7979b03fbd55856e2636c7e4c454b42539196b4187a26c63c5c6dce9ff22b381c7553b22ee45f5ae26658eab
132852e47cb1ce905ff1082e3c76d62e814e467ef3df5ac49b8d882d0cb62285a6095eeb2989e5287d1f3f189b937a907148225ef56322b50ea4d0bc69c650242f69b7cf5d911afe25e3ac20c7693d829d8d400d
8d881093fe7f20c7b223b626645fd533cbd79ba5ff6907567cfd96
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  c6da3a24d18255d8610b4bea08c6fd0f23aae637a2998ec7b1e0527a0f78fb254114350114ec6b6558ec824270ff6a3502c3ab9e0f09933
f6a76ec793de14951d82da815858b6319a133286750f690042d0262f1a41c675ca7a758d57eeff74490db221964a71e30db3336a94d1d1e32955bcc7e896078ebdcbcdbf9399ba082645f6042294ce658fbe6347
7ea21a2e3f94d387f6fbe12d238302fbf57b4281a3175e1beb90ca240ac9959cbb560c8b7390b9e77e3d808a911f20e837849bc98468c6694366329e75d588de9be95cc5619b5f11bda0d9fabf7a963b55608ee2
80bb2bd467617e638e10254d7dd4203bb011cd5c2bd9e638528ac471903844968
```

```
--------------------
Round  8
The prover sends a fixator to the verifier:  13fc661471b7e4fbcb7cd9b5e6c76ad32df6b79301bdb6c739ff23265f69e07b5e69029ccd600191af995bd789f6f9116ff767e8b3fbb6930d9e27d89e2
7ebbdc80c78c70417cb2494842944a86faf416261de06e5f414ba5f2f9d382fcbf5a8076bb0ece69b4a462247fd5e96abdaa00226aad1c2cc67b2315d668cb95d78d837ec8567b08c69eb5dda674f27b42fd3f84
c6eaf87035703265a36c3d6f77c2f817d452c8949d34de67f16295fcc585ad09db07fd280adb1759785c419707ebc2993e6c60b1ed682eee6259cc5883a65e1e01f935da2fa9a7054966a3ac1e95640920e38f8b
1c29f87213661373112a4132baa1a399bce1cf549c00b8fd3f2555
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  1bdb9aa6098ed02de4ffab1b43e4405ffca34dcb4f5c73241174620b82cdbb4a8f07ce6a0f0993d782ee79949fad92c84bb94171451af81
3c5090feef59f6f903554ba165c8c449f1178e7af26e067795ba1881a26510050f7cd6e807beb9b6b34ce76a1b4656f368d97eecf19d5263337081df713ef206827cd9c0343a4d9504e308d0278fd1f9eeb800cb
58fd347ace1c20c3a3cd5c7eacc91686f97acb47aff3a78778d3259d20a034282a78a3f3f3371f9a62004d10a7c46c3d3301459cda1dd543d446a9c4ee8fd6455e118d4717483b97de8ba538686e5eb8a953e4db
eac38f256da970cdd81b6cd49d0d685ffa39a1c03c39c769ee49b645107c259a5b
--------------------
Round  9
The prover sends a fixator to the verifier:  503121ab41c3f53cf5af77304ecc48682c29bb432ee405b086c8122d306b9a0f6d90cf934e14f55d16ce036397a2100127a6182e5ead8336a31f21f0ee0
69ec7c58beb53eb75d8d28a6d9f213e0ed6fff60e1ec3d3dbaa6e0720dc093fa31ee6db0df03d9c8d337c5adec6795447c1614b90ab03b9e86de1718d65be6a299bb2bec62a0e14f42bdc197fb892077fcd6738c
2a9ef248f38c3e2ab95cf3ae78dea3272d8a4038c4b0b1997ac311696644a584a8541edbd88444e197617650acf5d296967f0792f915dc84959397a265057c2ba217c03dd92cc612fb2e01830209072 0dc43015e
87c9a67cdf854d7924ce3c0c544bce05a42b33c07f596a4d9e67e
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  d142deed49892f33be0a5b39ce45ff6deb3a5a8b1da5412929c3362f55bdb4e8446ee26caba9e566fecfd05ddb7d6f425266ec2c9956b34
3a3cb98be7440708216087ec97ef39ec7b9189ab3f8a25875457c372f3cae8b10e4c9edfb10b1422ae62466a1f2973f7b68f414aaf953b980620529232d5439ff1c1274d1ff1cdb3b3362a4d48715ab64201bdfb
c479babe2e38b84e29321246c3f56bf06df2b4ea48a5e6626caaeff527e6d3c82a0ad7ea41d66ba7abbec31ce159327e4663555210be9efaa22f31b90623c5d6cc59e982a8242d9fa31fe78ecabf3f9be6307c49
3b84d11763290583115653b5c60dbbe24cba3990ead30bb6dbbdaefe30bde6ede
```

```
--------------------
Round  10
The prover sends a fixator to the verifier:  1e288e55d0d1f2cb7d458c54a29de3a316b24e7978ff2f990963d3e7863f8becd46f1c8ebb7ccaf773de853f7380fa5249b95aa6f759de935e02a800b0a
ba1ee5dbf80097f5f8ca6121bedfb2c3bc77dab1aa8b6025d5f0f6cb5a26b28db7747bdf52386a948bb65bfcfc84b2a6c298910aa253965afb926441866f894c338a985ff6a575f42261655678d119e1d9af9904
2f2ff29205123438f17ffc7780580c187732cd46b3508be6ca34d225559913e210639838a11d72da5da6e192f6d0824288a88ec506c52a26b6b7af6b205303e5c05d4f63b1f12ded32600358db6b834c282362d8
e6d818cbfbcd9946774c342887256d1ba727d89831927017 2d131d
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  1f51f3b3faa591a9062894588a08809b22d9106f690a69c050933a2db5d13dc56f6604b362948a133f51ba369098a9496739106c379376
8647bf1f8f0a11793a269cdbe6336985bb6bf86466e2cbaef398055944617c58edca4775f9bff1f57ca503a88c9cf7b0a87907dc0a46764f0b7c6b54e52d65fc6eca64796fc47b3e1fc004b75857e8f0c7a34b8c
1eedb856020877b79053204dcb943e326645cfba0ce09c8f5f1d17f719b6ec533cf9a1d2cbe24f40760a79a72ccc7ea911a096cda6b91766ca22e94a9e16771c0733aad1c1f0ae00db8f04d531cab4ff5d49fc3a
11d4f9be2527973e94bcca66cad44d580e0f0e178e088526e0e24ff50edeb531a5
--------------------
Round  11
The prover sends a fixator to the verifier:  7c32f018be5a1fd3da3bec04b12f2317a9c4a999baa5d0a11b4286072dc813e082abb889f479739080d3d69cfd09fdb27994ef9b610b590313001e39eb2
7182fe63f64f8d3b401e104e935050e6bf3ab47a7bae25044ceeaf5b41167c6577b570efceba9b5d8f675a4b034f64c1fb2654d07461d963747e3c1bb6d51fa71c58bb59974876dde08a986e099b851b79677649
61b61f43aa6861068d107c905b04604ff386ce941fb5b9a51f60cf7dc6337290e533a80344891be763a14e871e628217116ecbd5ba05bb494b7faead0f13bf7a48e2f10b17f0c70529ed9c200491bc8207197ddb
930ea875d5927f6ff1197f5c9a2393baddd82380d09f180688b1
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  682552deebb85fa521b2be1076b1e16227f8ffbc98b26e4755f4e9418bb355bec1128a5799965f52d7012e0c5d4376753556f553f7c5c0c
e6bc9a045beda482b9ba22d062ec3529b978b900266cd04be0681c72f872cfd0f092b2e69efb0a38b8d98ce8caf035c1f5aa60e827ccee6521b506de195ae63baf1a569e269f26d8482bb8374c6c42d9e4c61748
dceb86a731fb3d99b8c37cc76fab849ae9c57346bc025a148fbe7db99bce60ec72f0c75ec24f648aaebeaebe6ec30a1f83cbeeb8eeb6747e79beb1e66437692851d2b68c2f556e29c8e8cd075791d40fde2fa77d
78727cf3b53e573d1d6db30c9bf885dc808406a5a6708643631798228bff86188
--------------------
Round  12
The prover sends a fixator to the verifier:  10872 3b0078fda30c9d899b9b3ff097b47b89936c4d6466f5df29418291a0e17c86844799adcf48fc352d986c07300d0567a4734872d92c0b1a6bfc6ac1
a53150b3b05a10bccdcb6c605928d9536e29a703218333132394e9ee1d697c30296ba9fd0b15608ab95d9bb0ad838b602d98c92ce7b5afb6201addda4d92e736d5ded818bd1424df512613fc970c117a9301a8aec
6d5b6664d9a0e37be3812910fc628919be98dc25e31c71799aa39c73e5270410f101fb0ebebf6ac63d25872a55fb9df6385b1e1822337ca3f3bcfb9ea5507086004cecd7c70f358bcb5fc002e7cdba9f2627a4ff
e8c91a0232e9b16847d55d86f954c2ceed76560a4df429efcb9809
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  226c8f5b738aaf0a75f60ded046036e47730184023cd7b8c97d1b696169a8584d913ac7b8bc0f2fa0503b0ad3deec4f582eb646fef17aa8
```

```
--------------------
Round  13
The prover sends a fixator to the verifier:  c59ad9d34968c5225bceb4417c309799a6ff53f7628b8994cb95eed4bb961c2f9f8a02cf980b9ff3f6c482060d3e4b3981836035a3059f36201e8a1b5cc
d24dda66749077be5227330be3f0d79fa35f62a9d1678eca7498c40a7dc7851d83dca1a4992b433aa72f59e4facc2cbeaf99f084b7d989d6b4871c7a195f272d5b8ae8734f7a49e583b763b5e1353bef6049766f
d77a842170ebecdc285d84f4693df746979d94f37d7a6dd6aabd16d0edee7945dae360a9d55ab2d17ed401202a8820f6f8e279889764da287528fb839941f27e2a7d6ce27aa3cfdc9155bc46f1ddc383460b1621
50bd56e9a9cde1478313c6ffdac050c8063b0a2a06114f99dd82c
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  11fc7139d6644cb8375c6a30cb2956403ab4e3d5eab4a7dae60be75be380c37f8c6eddf1e9c6963c4393588038268e5453443cbd9879b0c
33e5732907d67abda384e7030d6e7c044b44567a649873ca08caabae37894b92ff2a5612393a49db168e52e6f6ce3bf4e5a98501433fc6d73a089443eaab5b320691746c9a25eab25028091bb23b7ba05953521b
b4e0805866d2ce8a7508d3722f9d83e06917e6e7d300ecfcf62a4a954806d9f33380bd0b169b2de79e4f77dedd6577b692f9c9da27b6fd99cbd29035922d0f96472afb599a6308ffebaf2513ff08a8b9bbe74b33
233c904590355cce2643efea2d8a05390cf906651f521c418a77ca68d7f38baa88
--------------------
Round  14
The prover sends a fixator to the verifier:  1a95caa24788e9fd9ff2184f0816ca53219d32f000f5914b8b12006f9ee4148c5a8528fee8feb1776f1f91dc3fdc679aa928c5e497044a119b6a1a7c3e4
50060f6034fb924c461fc6777f0a0948ba09ed2f9a353cae3b96f3bcb0e6e79eae40856c8790461b3752a14cb7f462c56d4cbe077f28167f829383d72b539cf15aae72b1a3e30dd7e480a07c7c379cd681a098c7
acc15fda6853018f8ab1c1471a0639b91e18f215cf705f6528b162fa7ca17fcbc14e577ce3c2b7bbb1e2233c4d29c6d9ec496cf9773648a8936e158aea5930842951acfc0067ed051fbb783ef53ec5669eba6f9
e74112dd9dcdb6149a09546b699b15541a22cfa6b2c1a67e1b302
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  1ac20cf5d1b637337e2ac24856d39f4d1b6e166ed8a9721efe77ecc4d640ca74b4e86bdabf8abffb80942bf06e01a1a584dcfad31702642
4c68de20a203f97a7f147fb340919cee4ad65d6008bcfa7d914fd9dfa78953f96046ba483582e770fb46fabc31a42420bdb66efcd42ef1b01cd74c720bedb6afa0a783d9e59d4dce771b35b85005cd18ae905167
```

```
--------------------
Round  15
The prover sends a fixator to the verifier:  8ef01e923164947b5f569d6a5616b5eba9b4e77eb47ea17dfa4a0e426b34ff0a18132e79cebadeac54841aaa3a39ae05b0eb59fce3cebee484d973c258d
d5a4ed246a6d3810346f3cd7fae068c9a75829fafea852eadd65258370lc944180ca610a72dab1eebf484673f7c87d816dff2ceff1e4a4be33b2d887c92055d7f91de42107339e2e2405c780e014857f43591b4b
f13b598dc0561aac6a17d7a35de7f15e6c1c19cf4a101be4df1b0e048fc08433f7af0c135becc47f295c2d78f454e48c72e7c83d614beeadd84f337b1053011cb5099ddb9be337f7e59b359b00d45b12201c84e1
604f1f48882cbcf1563c18eb95cbabf11caa3fdc0a0a9c7cadd85
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  859b24ada32e916aeb5462b6ba71c3cf8834cbc076c8d52f7bbaee69e7754e09c205c1464eaa64c3757d777dcef5990717a1de5d0893ebe
ac6dd284109576fd5c35cfac3ca334bd13d45cd928321993e20e2d9245b2f864aaef7dfe7e844b4b5563a151eef56e60afb32971ae6a50b5ebd3bf343ea46aef194f6132f1f461e7c842443ee5475b90418d8cff
140718ffd2f175f86cc9f287fcc950682e7b54cc24fc64a33939d1ab96b67a915e4498570e75babbbc484990bce1112a07cf473be1a920a0ee04e455b82b882bb8009b54282067d19316306c2157117d9998c393
c8527ab6e892c725b9aeb99257ea68e463efb93d7febdca649819eb021fbb890a
--------------------
Round  16
The prover sends a fixator to the verifier:  c4bf08659a3ccd644b6ba09354dae78c51f2ff19b0b4c25c463e6d84d6afded1c2c1f693f1e388ae80b5aeffc99110b487d09c72db94d2a577158a39c33
aa62afa873e0465fb016ecd5a1ba634a618d57fefc9c5a5962859c989a222cc2f1c5e6116343ef15fbd27bd7cd1e8ead4679489d81da82ce8ab1b4271425ab479acd930c7c0d7e316ba0f3d5d69a578967527e78
73d10a12a84c5ec0389fd31e98fccd0b7b2e54e583e0a100b670c995f43b97eca0963f49e5e0e8b11f060328a14a4359da2d94b1930f20f485cda07a9f1221e6a2ddb64a1fbf0936186942c8d6b034fd43a4f10e
0035463f4b10f4b79ef5db8eae763c195e4d9a7f97ef1bd4d90ad
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  a011e618b6da48c39787767ae919e2baa5831eeeea41905948c395a4604f42c3401e0acff4c0f4ac1fc15db9d4a1ba9bc7240edc83600fc
3bd4543df80edda3a145703a7a57058140367cbba40d94947318ae958221eda2453157995cc4d6b779b02a84c98302ef34484c00ae58bd96fc18f3e6733a9d13ab37fc2ee0e87ccc1edf55164600526f71e588d0
ef7f868dc42445707113 4e2d6d95aefd9af418d08e56d4518f1acb11a42647339f4006c98b7ebe29d8c1e23e77aab961a782ac987d18ffacbf50f192c27675c1cc8d19656455b2de4eaab1b44b40dc3e3b9c712c
5868f0b85b12dcf341bfe0fa1c91979aff920189e00ab748de43cfba5bb51495
--------------------
Round  17
The prover sends a fixator to the verifier:  54346f2d22cce6893436c21347b745f05c7a088b45e1726b118a580f5ec9e639485d800b37523babaf06da56bf4dee05234e12845ff537a9d3582966147
f89425ab2578a4e68f004b1936ff83fafe65fbb37d46a4c995d06777e5c549281d41c2096037c545fdf8896573d13a755e83fdd492419cce2f5133818387071bf8f02111ba32e7557d3e86f9bc0fbb4e855a5d7b
33fe868cd4fa9ba669ccdeb389863892ef7734fed6d4cd42ae09e59a07f9d2154076e95a7d08509ff583c56251f95f61c76cc72abd1576853fd88d5505aac76acce21d295419f7541396002a94c09783bc3f730a
5f4e63a4a80ed9414dc28118fce94097d639009d7117f65d3a41e
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  1de2b2f0f2339f0a80e095d4a4a805772bfc50fcaf1307a3a851fa916f280a5358c4227b5f9f06e1a42c58e2eaf5cfda26c26a86dee9ed3
b41bfc8f3ac75844a808e98878f4eaef54c76d7426a4506976e61856cfc881906f436b0ccdb5ccf0418d82863e944e4f1135c1c265635e4b81e7c818b4707888cf33ce212d05264444b51e758778301a4e696055
eb77f27001389742457231 36e6e3f7367ce661d7fb444dcd32d8722993fad29ad4b1d04859c2d4a29d530b66921746e6ad1f4ce3d755b6380b6979c6e437bcfe56d2d68cc251c2ee2ea3a98e9e86184ff1ee5a09
622230f6cd0edf4f4fd5feb6bc5ed7a9faf8c190561753121d5ca5b8420dc8536b
--------------------
Round  18
The prover sends a fixator to the verifier:  1f486f3f73a88f3a94c7af8ccfcbd79f6ee3e0eeb63fa199edceaf68667527376306bbe30fec4b2842f9ed56071ff8307eff1d1838d1209929d767f581d
9464335042de3f1aedfa6e4fe387e35f02a0bfdef39d097334a7c23accab56addff1bb0d95a22cb9291871ef721be22f1e0e74bb5f19b137b33f494b2ff15199faec1e7b2735a2b45f40c565fbba1be82ad7b974
2aa70721369ef43877e795a3f79bbdaf341ff74f68cdc35f2a3c69975274365cf493b2a3db9a5f21485f10bd8833f70812f61c44a66b786b74f7ba2f4031dd03d7828f289e1e2f91bd5c7b0df84110069b4d7949
8d582cf2fb998eaf82fb03334e193858f298ae7f62a54928ea83b4
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  1ba08142cb946ef789dbca8208b6c5db58b4add46bca83782e58d5088623faa4e0dd4c67afa315297c063fdadc963984908454cf763171d
```

```
--------------------
Round  19
The prover sends a fixator to the verifier:  5be670931aa3d5e99a48539dc78dbdefc95d305fcf12aba47ddc4a2246b5eb8e28a60025fc72eb56dd45f72f7441bd8db04090799b41a3e7178ad9c052c
9def7f4fb0d2dbb1b2d364f263d4c3da398294fe4475535cca1a012eac7838d13436ae864fc7ab4c714a9ae324e5fa40241adb72455a7715926358ca131ed004a141d64beb84c8966f210c0d2d4ce5aad28a70c7
1a0ba7e977d33333a20958208070f11202bbfc4b55fbc9f8e1707162222ead57bf0d7b885fa27271984cf8e13fbe6498ba2de1e183c2fc46e158d5b90403dd8738913bf9ef47bd38914b6d31959032b813db1c0
927ddfd1a034fc64091287a23c6643ed4e8616bf404a436e1f9b
Verifier sent r = 0
Prover sendsthe value to the verifier for verification:  ce2eee7f179d9e956c7d6c8de1c6dc6ddf32b75a95d4a1a9a285f3ae34d2c69766a3b5aef06da224e71fa0b4a955f257416bb671e47ed6b
a55caee8f7969ade99f8c5622c26024653ed008a04325ef005c7560ef03b68bcd2ded8f9d58f08de1feda462eec82d647ee06813f7266341ecf9a719234695b3adb3dfa35fb6e6f0555363b0848c527496cdf487
86cf8d43c6391480d03e53c7e8c767f457d9807ff1d39ed623b5ce3ba0d5f356c1f140f0c6420723d00b4a67c82e3712860e9357f3506fee134194e8035d7788916188675 6f5f16e922034f81211b57b2defd3de
e5c1c3e92d60d93641037d09c4361607d990d41a2689cddd9bf1ff5be42a3c55a
--------------------
Round  20
The prover sends a fixator to the verifier:  16120d8689883ddace7d5852c21d02e6f663cba42af752d6a9f960f511165e2270c5c9cc978339043e3840d04885dd8dcf56ff7796a20011abb7f34006f
d8440da2588140d2c092c51ace7d61a6ed1696775f4bb30a25f02a8ef5fe18736fd63233c6a0a43ce26d665e8f7810396ce9163fd88845504b948dcd79558a47bfcfefa3da4309cd79b601213c89e069835ae802
673171687bfa3d52ccc86e95b5bf776cf6d9b423e72f443de7b13c5ba6bf8b97c6f05011f5eb57b7a2765d40e9b5923b09199e2709a6de8beaca8898aa22e96de6afb674fb2ba28ca586a9ae7273ed0187878259
f00e5645c987d94fffe839169bdd042da9b3f13a0046336251bfd5
Verifier sent r = 1
Prover sendsthe value to the verifier for verification:  5d9d0b787e36a4e224094cad4003a8b9053d0d43b9b8027200b74690cc7f9e993211972201df744e8edcb6cd4569c75bd38bdbdf49f9c42
d152a5d04acfc11d830c5ebb4bb6505d06bb6415c95737bdf4aac0390b806300c8e6caa3bb742e40a003ff36ba4818c5cf8a3ad91d205f4ec79d1436e512af775d77ad47ba3406cd6b8eb436dc8f611de93014a6
23d55503ca7d612dd1ba7ab60aea8704f5c4926d5cc56ca31b0044596e6fb1a39dfa3d45782d174759d899cc4ccd5c74f944f995b024761fe2cb5273beab5821367769fd39502dadc4cbeb8f8963c45a6fa23780
a76ff1ce4a760bd3e76c4297f12eb6f21376045d5212be5e01c3aafbaa68a3ad4
--------------------
Check ok
```

Вывод:

В ходе выполнения лабораторной работы была реализована процедура, составляющая протокол доказательства с нулевым разглашением секрета Фиата-Шамира. Была написана программа, выполняющая математические действия, в соответствии с протоколом. Также были рассмотрены возможные

действия нарушителя и доказана невозможность прохождения проверки нарушителем.

Список используемой литературы

1. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург, 2005. — 288 с.: ил.

2. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: БХВ-Петербург, 2010. – 304 с.: ил. – (Учебное пособие)