Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №4

Виконали:
Студентка групи ФБ-82
Муртазіна Аміна
Студент групи ФБ-84
Вацик Максим

Перевірив:
Чорний О.М.

Київ - 2020

Мета комп’ютерного практикуму

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Постановка задачі

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.
2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і p_1 , q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \le p_1q_1$; p і q – прості числа для побудови ключів абонента A, p_1 і q_1 – абонента B.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d , p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , (e , n) та секретні d і d .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$.

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою http://asymcryptwebservice.appspot.com/?section=rsa.

Хід роботи

1. Як відомо, для сильнішого протистояння криптоаналітичним атакам на ключ RSA кращим варіантом буде запезпечення наступних рівностей: p=2p′+1, q=2q′+1, де p′,q′,p,q – прості. Реалізація даної лабораторної роботи була з використанням мови програмування Python з використанням вбудованого генератора псевдовипадкових чисел *random.randrange()*. Таким чином, функція, що повертає просте число, перевіривши його на простоту за допомогою тесту Міллера-Рабіна та попередньою операцією ділення, матиме наступний вигляд:

```python
def gen_prime(num, s):
    while True:
        _p = random.randrange(pow(2, s - 2), pow(2, s - 1))
        if test_by_div(_p):
            if miller_rabin(_p):
                p = 2 * _p + 1
                if test_by_div(p):
                    if miller_rabin(p):
                        return p
                    else:
                        print(f'[-] {num} failed Miller Rabin test: {hex(_p)}', file=logfile)
                else:
                    print(f'[-] {num} divides by simple primes: {hex(_p)}', file=logfile)
            else:
                print(f'[-] {num}\' failed Miller Rabin test: {hex(_p)}', file=logfile)
        else:
            print(f'[-] {num}\' divides by simple primes: {hex(_p)}', file=logfile)
```

2. Генерація пар p, q та p′, q′ відбувалась наступним чином(більш детально в файлі rsa_log.txt):

```
[*] Generating p:
[-] p' failed Miller Rabin test: 0x73a118c4b69cf7b3728dd2ff1c54dc606c9ac563e808cfc261bf83acd8df98b1
[-] p' divides by simple primes: 0x4e3be2e30fe4262ed2cbba833205bcac4cbc9c768ff620b18494ed50e1d5ea7c
[-] p' divides by simple primes: 0x50ad559549ddd0702aeda2132fe61be94eb7f8fb35957053a3e897bf899e9ac4
[-] p' divides by simple primes: 0x68611e705ced320b96194618630da3166743100f7a0ea4be0ade431c902cbee6
[-] p' divides by simple primes: 0x553afa69d065ae6bc79ad259b91ac7e567d44edf24c010c19bd8802177f8cafa
[-] p' divides by simple primes: 0x55c4fce9de26fbd87fd49771a5d567ab1e9a5fcb86f90e975bd3870017cb73e8
[-] p' divides by simple primes: 0x7ef37f5dc2518fefac22e79a8254ed5a7efe4b2518f2eddf7f7a2729219c2e30
[-] p' divides by simple primes: 0x56f2ba4b49e2abbde39f750a77c4c4aedbd6f1b3573cdeded1da70340711951d
[-] p' divides by simple primes: 0x40cf85e3b2d98a51f4a3a7bf677c3fafdc656d16e08e089119e29da4d58e7922
[-] p' divides by simple primes: 0x594add146cde66f61f0af70a749c6db269a831ad8ae93904647e24dbaeace529
[-] p' divides by simple primes: 0x41e2d6c78ca24c191742bac0ce9eaa687cdc056150607e216c14ba51c4fc43fa
[-] p' divides by simple primes: 0x444d7f424b2d8ceaf68a9ea1cd24d6ac677b7d8552cacb4574b58f4991f33a0d
[-] p' divides by simple primes: 0x66949ccf64276b85acf26c6b8f5592ca7b2247b97249074da5564b865ee78996
[-] p' divides by simple primes: 0x4f687131086dbf606a498891c7a624b3fd2321c00d306dabc4ec5ea0e1bfce7e
[-] p' divides by simple primes: 0x6cbce337b4a408cbb5a0d5d49fbef88a26aa2460a8c519f610a2575a09824c35
[-] p' divides by simple primes: 0x7d7d13caf5d06def1128b0214ae2ec58037f04cb56b4c40a59ef80f3a591e1c2
[-] p' divides by simple primes: 0x429730d667f4937217cf86723f117e1331cacc91976893f75822f3a542d0d6e4
[-] p' divides by simple primes: 0x6fe9a78bfbb3b84244c2c8449162ce883581a2f5a17cb30fee813a5162c300a6
[-] p' divides by simple primes: 0x7501d5690ad8f8a42e7400c7a9ce62bd85c069aed012b802d024210c6cfe9c5f
[-] p' divides by simple primes: 0x45a7a5ee08bec0028b5cbe9e22f2f50ae75680cf2dfb5e8d8521fc33396a6899
[-] p' divides by simple primes: 0x56921c907a46376c7e67517611745788636ccae6616dfa6c3e1e72876a24fba3
[-] p' divides by simple primes: 0x662ee06c0fc1534899a46a4b8dc08622e857a7c224126e3c91b58f4308bac156
[-] p' divides by simple primes: 0x7696dcaf341df70e753b6a13f86b9ef85a87858c768868cbef8f57daabd8e449
[-] p' divides by simple primes: 0x6414a283853c57b95b4e55688a79d0cc26f78c6ef72f67dbf08726cfce626b9e
[-] p' divides by simple primes: 0x6203493c5cf36b8dacd772e3da8189eb650026efad14bec39e4a5e1e6a31de32
[-] p divides by simple primes: 0x6f6a57844855174a49bd2e1453ddf00120034c1954c4386aa8d30066de509ccf
[-] p' divides by simple primes: 0x721bc76512b728ae9b0297d62fe2f48194f4d8bd5bf820e9b657fcb59144493b
[-] p' divides by simple primes: 0x73486a050325456f659a533afadf14783702f266ea40b4e45f3926d75bf8c093
[-] p' failed Miller Rabin test: 0x43610bead1c9685b4ae19d2a13864db09d520c526406111612611931bcaf4241
[-] p' divides by simple primes: 0x6939334a74d66373ecf59c517eb40461d4c6f014629b7757be36845b90d73918
[-] p' divides by simple primes: 0x5261cc1a5f7c0ebd3cae71171fc3f1d132049ce8e5aff57c97ad96269f4020f5
[-] p' divides by simple primes: 0x72536241ce0a61dc3a9b9ddd72e3d971333d8a439bf9402653c34b3a5925bd3a
[-] p' divides by simple primes: 0x42f63f0a53493d748f809986483001d2b5d470b7383038401d6f4d5a0fae17bb
[-] p' divides by simple primes: 0x51d9759c5e7569fc820114e9d96fe7b526ac785884b06afbdd2421a7fbeb0ccd
[-] p' divides by simple primes: 0x63c94e9971161432c31bc1b922613ac3ed4a884f75dab25f43af6db87f7cffec
[-] p' divides by simple primes: 0x445e1b6184ae56351994bdbe13b0526c874a84a9337aa2752ebfaa37c2567c02
```

```
[-] p' divides by simple primes: 0x58adaa256bcad8789585e5d2c4e474062dbb6d63e355f648cf930e38ad3f7904
[-] p' divides by simple primes: 0x76fca656710e65f13e78ac9903cc513d85bc92eba1090e44107463c2a3f75e1f
[-] p' divides by simple primes: 0x5c0dc0a341874aa11df059ef0c39c4d0c90dbba15a188d9a903e604222fb31a3
[-] p' divides by simple primes: 0x7d8fed0cabb6dc0f1ec8cc222927132e34f08772fd796847c31ba058281695b5
[-] p' divides by simple primes: 0x5adea7c5790895ae69540ee539079ff0a25206250dc2bf736bedef08a720de82
[-] p' divides by simple primes: 0x4ca5ec09bc5390817461721aa39bed95c482f41a688dc9a4032c865eedd16692
[-] p' divides by simple primes: 0x708f04eb3145b39ac7273f556c304a40c1dc06b3fff3ea3c802843f5c8643394
[-] p' divides by simple primes: 0x5d0e871383e5a6eea8a5a8f7c1f47194acb68db91564e812ee9dece958d877e8
[-] p failed Miller Rabin test: 0x72fc3af2d7845222b7f3d111b34230380877db18ea906c233b291e244eff9edd
[-] p' failed Miller Rabin test: 0x54b7844db12aad3d4aa46a07f4f3583f44afbca465da79d6643a87713456f91d
[-] p' failed Miller Rabin test: 0x65c2e092c55da7a134fb11b19f57c4b0591df48861ccc68061faef531edf17c7
[-] p' divides by simple primes: 0x4ed6069c1213c7ca5da3f79ceb790035b4b4c944c4455e473ba0e0fc28a8a744
[-] p' divides by simple primes: 0x571f72ff6c17ea810eacd2da9a0a3629f8b5f7c6b6ed6fa563c8ae72e3a4f6bb
[-] p' divides by simple primes: 0x59ab14f076d244c60b433d7da1acb473e59313581c38d0148cf946118d9c2293
[-] p' divides by simple primes: 0x7e7f653b4f773958600662715cfafb510f9424ca572c6a0e112fdf55de8a5494
[-] p' failed Miller Rabin test: 0x5662114c46f88c733fb87ecd97771cbcc8c0421c3a54c001de5ad66195a2e069
[-] p' divides by simple primes: 0x7c847709715af0e7c918aa8756d48b83bda271502ae126c894f059937bd3c7ff
[-] p' divides by simple primes: 0x6fbbe31dfec593da4f8d4447bb47d757b84f3cf6cfa8c9c8863588fd5d7cd20d
[-] p' divides by simple primes: 0x66de638c53a83d7576ba99e9686ea7b24a2410cb1ef59c8a59a2a58315d54e93
[-] p' divides by simple primes: 0x4024806b0d2774df3560402504744e954558fd4f73ee9cbfb8ae4acbaa4da7ec
[-] p' divides by simple primes: 0x743bccf26409507e87dde9471592d2c01c2fdf895dc970442c9e5d7a7d6c18ff
[-] p' divides by simple primes: 0x42ff92af62873392b00846cf198efc55414d872951dd935730c54178ba0d0943
[-] p' divides by simple primes: 0x50527a41bb37896b9674dfb7b75044aa25e8b642f19ec714a93c7382ec881e65
[-] p' divides by simple primes: 0x7f567b5b964e000d193e3b90b712b81179e90f7bc66fc37a0dae40a8507fc7ee
[-] p' divides by simple primes: 0x71b8eb261353dc62401c107292cd26cf06a8e934b48eb2c5d2c1e82b2b4d415e
[-] p' divides by simple primes: 0x4c298a66b39ffca52b76b70f6e980bbd355bfe1b25455f594a1e6a576e4f1fd1
[-] p' divides by simple primes: 0x77a45af6246e0eb8a6748d63663a4d7fa87f6eec40893ea04c70b5b3352bd6e4
[-] p' divides by simple primes: 0x7eb563375b5b3434caf7bef89e1f7e8d494b90ce49d3e7303812ea1f1aa5fdfc
[-] p' failed Miller Rabin test: 0x7a738e1d8a25c354668aaf8802052320ae6723f8cedf41f3271e880525e387c1
[-] p' failed Miller Rabin test: 0x4c90e6a05ed31e512c173a4435efd23a75b90ed0669e13332ebcc7d2aec897e9
[-] p' divides by simple primes: 0x676eaeffc3157a4ff188618a873eae3ebd829cf9f7eeb997b33e7f11245f260a
[-] p' failed Miller Rabin test: 0x6594913fa5d3bfbb7eeda2c306343d475bd316efab4a41b7f57d3e0948163115
[-] p' divides by simple primes: 0x6aa4e874e523484fde316cb0852499e646049f75ea0f65ea1a8db7f4dae9ca91
[-] p' divides by simple primes: 0x4d56db037d07b72f0cf06be3eaa8c086f010fdadb3575f60dae8a098cd4eeadf
[-] p' divides by simple primes: 0x63d7474c9932ffa077e0bb23510e2f376c7e416c1c005e54c169c8a812fb1fad
[-] p' divides by simple primes: 0x74dd53df806842e0b0a804ce18af85539aeaf6b70e327acb57b1c1a38cbc8db8
[-] p' failed Miller Rabin test: 0x4702fe2c041af653a361c94043e3988de435b195b425fce626cac6156db12b89
[-] p' divides by simple primes: 0x7cde40a6b0f2b3a4c389fce20d1746c985b45be21c89fb750166535b718e1663
[-] p' divides by simple primes: 0x7894a243fcd1b3357741a324baf0e5d4d38de9030a28c47d0156a05428074ca9
[-] p' divides by simple primes: 0x4654405fb37cd851720e91570d029cad607e82ad01a8582da17d30bee29ed736
[-] p' divides by simple primes: 0x66cc612cb17765e0232d18e1f10b957bc7fc753a101035cd9a903b05186e396a
[-] p' divides by simple primes: 0x7479f8e9e527a966254c1d8a2f13c75c3b828c5930d48d3619e552769c5abeaf
[-] p' divides by simple primes: 0x59528f2877ef553eea8e8b7cc8f8ab1d72e5c0533b1b64c4c309a64d136a171b
[-] p' divides by simple primes: 0x6ecfc90020cfc1e872450cd7a53bb7a6b99788c566250a1c8fbbf9143eaae2b4
[-] p' divides by simple primes: 0x7fbc6369acab9096927eb531b3101ed36b00935cf7a3cb28331387634b793959
[-] p divides by simple primes: 0x486c21db25926e782be6bc5737d695955d4a97ebe5b68b8f0afb27a5c00849b3
[-] p' divides by simple primes: 0x59dea683cbb7dca3f9a76709d0f11d61383cdd4ec1733a7c2fe6156985b3f8d6
[-] p' divides by simple primes: 0x5223d34264dc76c1945f5b1a21f0fb380e9e37fc50ac7825406033e8173591f2
[-] p' divides by simple primes: 0x76cd8ceb365242bdf3be96debf70cbf8070b2b9b368c8f1ef45f5b923b43b51e
[-] p' divides by simple primes: 0x5b30c111bd0498fbe759ed46a568eb89496560680cedd1689aa97090d29e4784
[-] p' divides by simple primes: 0x5a4443ffa7cfd2a6cca82ba71c6b4031498e00399173bb46bbb76174fbf67c79
[-] p' divides by simple primes: 0x662b567a02a124e9a2d05b5fa5d45413053d5023c2e9f68c9bf91a852afc9f00
[-] p' divides by simple primes: 0x5ed4d2b6f3331ef140bbd017c5e8ac83e84b6ea7abcd9f5dbb759a60a2803bb1
[-] p' divides by simple primes: 0x69033a11064188c51e3ddbde27d65ff5a2547fd1c7fd24977445970ab4c4bfae
[-] p' divides by simple primes: 0x6e7f30df03f6492225d358d3bed1f5d7b2fe60927b7ecfd75d5f80afa5571f7b
[-] p' divides by simple primes: 0x727b2a23de9961724336afb8be24d821cf1192d44bf345b78b9f74286537050a
[-] p' divides by simple primes: 0x6ef10c83aeee0ade716b372906667397ccb0f3cca14e5ff340767b98f96f550c
[-] p' divides by simple primes: 0x6e2c9812a96c9301aa89a2c5f747e377b4cd3445a620b405cdf850ba7c6ace95
[-] p' failed Miller Rabin test: 0x7cf16d298c6e8be755f000cd3af07b6467e13a40a982a765f82a8d3be6a5b4e1
[-] p' divides by simple primes: 0x56bc630936edcf2f6bca97fdf60f078be6b58f704cc3b8240a2c0108ef499a3c
[-] p' divides by simple primes: 0x7c3b8059189f7321f2b9118f3c38e790df70e9e388cc295cf1290b0dc3905c19
[-] p' divides by simple primes: 0x6f3fd1bd93e76fa8b0f4bd47201344537a540c42bb4a1aaa8985b1d83faeec4c
[-] p' divides by simple primes: 0x57313eda710800e8a2fcce3f83ac93254de03a047dbd61ad8038cd5eab5628de
[-] p' divides by simple primes: 0x42cfe451824854bf4f3551c18d32717760a0db719d75fbc865735c833f09fbfc
[-] p' failed Miller Rabin test: 0x726b9e8a0183f5547ae45e7597ce68cac229bdb00477b17b2c4ba55d6ec61a0d
[-] p' divides by simple primes: 0x7e611dcd9b535874b76fed758538604508737 3a1c870c5b9494126f81bfb581
[-] p' divides by simple primes: 0x460cb4ffe4d72c53518d91dd714426fafc7fa7a6a60bd5405cf29e52c1f842a9
[-] p' divides by simple primes: 0x6dd12d08f463260aa5a950384809658d8fc29355b7f91ddced29209c30c21dcc
[-] p' divides by simple primes: 0x77e9a6ba5d5637dd14c7820cb13777b595304443a06a792df42591fbecdadcaf
[-] p' divides by simple primes: 0x7793787ea45747118d0ddbd868a1fd63e04013ba4d431cdb7cd449cd7b9ac0b6
[-] p' divides by simple primes: 0x5fe537965b202f444de214164c09cdba6864c6c3b7772414b65f3cd9b82377b4
[-] p' divides by simple primes: 0x6b7b46c2e3645820390ed7485b95b0f1edc52e4b98be098db5e1cb5601a41a67
[-] p' divides by simple primes: 0x45b40e38d92f9ee1872c8cb255e1adf0434c4c8a3659ff341ff0a4a89fc0d1c5
```

```
[-] p' divides by simple primes: 0x64c0df766da56d402777aac7e29edf6cf6a0382aab0441c32a3a559142c278d2
[-] p' divides by simple primes: 0x7c1e445afc923238e5eeafc2e1f7f869fb93bbb0543cb99e7bad8fe39076c7d9
[-] p' divides by simple primes: 0x46bc20bac49ebebce9a51e10fe425d8e29dae7064b5d125c835577fbddff6fd8
[-] p' divides by simple primes: 0x549364612c809ba7411d856b70b55ce9b0574bcebcfa6419ca88bede7365f38e
[-] p' divides by simple primes: 0x614a50d331088670c3087dc5432d2d759c7629ea49a5fb33018428b47f77af71
[-] p' divides by simple primes: 0x53a9414f23f2fd2357031dad2992ee3f44f226b61a23840c4cc1e560db12996a
[-] p' divides by simple primes: 0x58689b75506780653f5ab60bbfc171825cac1287df2bb6452deafa37c3622765
[-] p' divides by simple primes: 0x7fe677707da89290ec04c33a9d5bb64b64412b9bbc8aa1ef3b38c7c69c38d99b
[-] p failed Miller Rabin test: 0x672eb7be8dae07e2d35d1f75f3670369a9d0c981d8ccc34cb04b578ec6d51ac1
[-] p' divides by simple primes: 0x56847d917d720fe2830ff5a816c9164fc5ffe71cc7a35b25192f8abaae413f5d
[-] p' divides by simple primes: 0x7ed69c08d3bf18d8440596a281be491d94ef39981068cb445fc88d0ab2b0286a
[-] p' divides by simple primes: 0x771c84248b3f8cc56150e64a6b764abbc5fdbe49596b8ad7a7f2b72219acef7f
[-] p' divides by simple primes: 0x6283580012e54a79c4af8fbd953ee89785f55728db0525602fb51d066ffccc98
[-] p' divides by simple primes: 0x43e8aceecf89fafe13a3229eed63279056160294834cc1839e8e29a099e30b6f
[-] p' divides by simple primes: 0x4f1a07fbeaf4f654b9ea9a88301a1edf056da6fcf175c7093fa95734acafe825
[-] p' divides by simple primes: 0x6204999efc058d2d3e70c64fb57a554dcae6ddbce4702322368923fe07c516c7
[-] p' divides by simple primes: 0x43113912ec668c7d03d20593bf36fa2cd0f5068801fe51e199f536d6d236308c
[-] p' divides by simple primes: 0x6c9d09daf8a4ed23bb5b621d3600f7eec131929247763b2c771b51211007532c
[-] p' divides by simple primes: 0x7b4d8c93b82fc56569f201609b5d491e20e41e3fe9eb137066b5ae3752b9603a
[-] p' divides by simple primes: 0x5027b154992b9cd4ee5d01dabf05e73244b2f039e36a19c2f003b8f56c887326
[-] p' failed Miller Rabin test: 0x6f2feaa514f569e9fe194d5e32967379afced3f7a8a5a5904f0ce2e697d6e187
[-] p' divides by simple primes: 0x7ad99f1de3cb71f4fd88095015462c72a58164d30de8bc88c2d4c4ecf78c0c34
[-] p' divides by simple primes: 0x5dcb0dd7857a36d694d7a9ce8a619316307c7db613553a3ce333938228b9e022
[-] p' divides by simple primes: 0x683e5d9941755ffc15be19db95ecc3b86e281fad934890b65f5e48d431710853
[-] p' divides by simple primes: 0x77c98871bfe52a0fcfeaf7d8182ea77f5da54ef3f81143e4dd8984de3e8b7162
[-] p' divides by simple primes: 0x7dead0988bb6830ac250b95f6028daaf10a9a99a945ef076d0e240fb5e87bbbc
[-] p' divides by simple primes: 0x49a6f57f90446dfa4e163c3f06eadd37abb6e1c354b07cdc9bb681f076a55e74
[-] p' divides by simple primes: 0x537903f96a525e6a827dd55e5477a6769d2744efee4e030fdb730908e9a164c4
[-] p' divides by simple primes: 0x68d253d94796ba23d3e61b75b892d0a7cfdccf00a257dc525bda20400884e53a
[-] p' divides by simple primes: 0x7839e3154ab58ab901a0365c584d9ff84da0b019f8458042cb3097d0fcd8faac
[*] Generating q:
[-] q' divides by simple primes: 0x7fcab5e7e0830d123ef687e06826d9c4ab27f254d2aa4d8d04a03e4434516081
[-] q' divides by simple primes: 0x447c9aaad2bb705628306b64c821a7bf700a07c7ca20659ffa011b22d966ce38
[-] q' divides by simple primes: 0x42f2914d9fb635f1f9ae2ebe746f3b74230f2b1fbba4a35187495930dcd2e4c9
[-] q' divides by simple primes: 0x6c444481fadc13400d28992043f638cbc5ef0106fafe5d12fa8e88570befc7b3
[-] q' divides by simple primes: 0x6506822dccb3cafbc4f4b16f98afde5d213f4be0a8756ee87f8a2b54a1fb89d8
[-] q' divides by simple primes: 0x606a3c7ebd3901597bd973ff2a85dc51045a5c483154b16458130114db1f8737
[-] q' divides by simple primes: 0x4fba2ac7e958ac43111aa54aab8c4e1d159b879d1a64ce6286415b120f95f7aa
[-] q' divides by simple primes: 0x6d2c98edc1493f3070cd56b1a843499b1a6ee71684df1d20e92053a546bb1c4a
[-] q' divides by simple primes: 0x56fc79a406cb238c1d8242c4ed8b6ac4519af3279b83ae157fadb9d3b0218c79
[-] q' divides by simple primes: 0x4676c42f2f48f26a557873c108da1fc1821bea4c535d18245cbfbd38d3239ea9
[-] q' divides by simple primes: 0x777430cac0d26282b7153cef40ebc1af40865c2fc6db05cad911e86384686f22
[-] q' divides by simple primes: 0x7e0d1dfed4c2d06f40931ec28ef58d6b50bb1ec4cd1cf358c4fc0e6ac0713e93
[-] q' failed Miller Rabin test: 0x483326fce5c7feb7abe571c8123e25a1f41694e5f894c343472b3c7ca4ab96f5
[-] q' divides by simple primes: 0x6da4064ff07a72b454f1bb8302e5336a6ca23a8e44a3d41a9adc755a7e84529a
[-] q' divides by simple primes: 0x6696a739854ea16afb8b076d80760f4a806a1b737385b26770f8d9f4d848e455
[-] q' divides by simple primes: 0x6933d3e19414138734f3bd52fb035bcebad7ab81153dd248c7deccd0c6b7478e
[-] q' divides by simple primes: 0x7b1d673c77667e56ba95c3e92b3edf06fe942dd6bfa8d5644f33af98c646add6
[-] q' divides by simple primes: 0x6ae32b6729c8cbe7d984119e2137b69da5205506afe18d9ae6099562095a3afe
[-] q' divides by simple primes: 0x4f400149201eca926dc4427fa1d66c42e43946e2f830a502eb390a008b37b2f7
[-] q' divides by simple primes: 0x55853e599948bc57e607cf6d6620aadd47b92a43164f042fe4c66d2ef0059dc8
[-] q' divides by simple primes: 0x5ae8566112b06a185e78db14c9ba0e6ffe8612f977fa290c8a1ea2b3e9f9d782
[-] q' divides by simple primes: 0x4c9d05c5f3cc7d7004e1b9b861406c052493a64f1dbdb3132827aecfadb5c814
[-] q' divides by simple primes: 0x5b9bf2f47336aee8380d918acf9d6842889ab6ebecafd16695e6fd67ad2ab8dd
[-] q' divides by simple primes: 0x7b7dc0bf39644a39d58099e68c9350cf1426f79b5b18c2168c600d056af2a61b
[-] q' failed Miller Rabin test: 0x5aad3172b171c41d7a94d4eea43595710531dd845fcbf0ed3ed7d8dc56502155
[-] q' divides by simple primes: 0x5af8091d0351260deba98ef7b1a45026016775d484fba645705643f910f43cac
[-] q' failed Miller Rabin test: 0x60d0200340e8afcf0864716801dfb4ed7405ac73c561c4cb4f1d15623fe79bdb
[-] q' divides by simple primes: 0x44b5050b570ec6ce9d7beee9e3b6a13ab14c9de5110cfe340272ab2788e6e0b5
[-] q' divides by simple primes: 0x5d44005539ac659c751ba0628e75edc41861f6503b933c05770940529d77d354
[-] q' divides by simple primes: 0x7927e467d18a46aa313b98a0cb169b4ddb42641277a2d55397f7228f25d0cd48
[-] q' divides by simple primes: 0x535beb1a4085b89f6986b4cf3d8d9ec6ca11bb5b853851d02a8b224507a808ce
[-] q' divides by simple primes: 0x65c667e6c81e68815e8b4c195d140680bc90c99fee354e7dd43d4f545931fbea
[-] q' failed Miller Rabin test: 0x438adba840a86b60c845d3cd62de8eba6e73d4eed7b5a0380d595357b9808fb7
[-] q' failed Miller Rabin test: 0x60f27bbea401563625c858c920023ade61e631052f1d37f1a0ad8183bf3225ef
[-] q' divides by simple primes: 0x7f551f01a002ccd14ca7c25c46baf32b83132956de61fefe212928b18a640e46
[-] q' divides by simple primes: 0x4ff37ad20b55c03b2423dd6917582ec9246d9d726fe5664f614ab7519e581c27
[-] q' divides by simple primes: 0x5497c3ac5922fca08b14ea8cf92153e269f3ab699de9e1e95f04357a55efe1fe
[-] q' divides by simple primes: 0x75e98852a2ea588a7202cbd86f7497ad1874eb5fb46dd0537a6986a8d095151f
[-] q' divides by simple primes: 0x56828b4d6e515dee3648d02d2dbf55fa58ad3a75af8ffe24b1511df3e3f37b24
[-] q' divides by simple primes: 0x5717c3bef2fb9025a7f0b2252c391c2d56d35b20e0f9fac4d73d6bab8d74dfc8
[-] q' divides by simple primes: 0x70ceff742b4fff22982686a577a410cadb6bd0e459a2b1d2471f76f0f2b5a750
[-] q' divides by simple primes: 0x40194bea16beb5f83e1a0f51a2a60e63fee928a7f0218a82c5b0bc5779ef38b7
```

```
[-] q' divides by simple primes: 0x4282d0d36b71498cccea167c96e1de8b9ba8c02a80cc21283b751f79e451f2e4
[-] q' failed Miller Rabin test: 0x4146627ca2aa62b8c208a81ce8dcf135a8feefcece86a5a288ed8efb51a201f7
[-] q' divides by simple primes: 0x618b277bbdb552a34de39d2c65abcff60b25af200eb98f43451eb352f76ca875
[-] q' divides by simple primes: 0x5ee82da3613f09ad5d3a8fc2e764acd3c265ea1c4a60bbb02023eedb834a0e5d
[-] q' failed Miller Rabin test: 0x6afb4167614d9760d17587fe5a9dfa62343c3ab027a7944dec3932f3d0e69dc3
[-] q' divides by simple primes: 0x569b5bdc94927f99ba70f4ee88896adaa750ff33d4a4bbb3cffb451e203b0f8f
[-] q' divides by simple primes: 0x635f5ad9148bce6c0a72a7a61e982f13821fbb7ac585aaeee88ecc83d78ce767
[-] q' divides by simple primes: 0x5f73c4e379aa276e4408823c904d9feede08ff34e8f34147256ab281bf343ca2
[-] q' divides by simple primes: 0x44c46398f78cd09ae133d2416a58d4074e19c9dc351789475a0a0e15938b0762
[-] q' divides by simple primes: 0x64bfcc4204b4710aa43c4ad249ea422ee8e0f419c05ac6c9f9c9c9c5564d5160
[-] q' divides by simple primes: 0x5eab9fa9e572d1682c0b19050b60560ad16963728b8f4be2eba93024682821cc
[-] q' divides by simple primes: 0x7fd26085aaa8ba1d4b92063eb9c051a4abb84715af5f2d37cb98fc24cdb6fb4d
[-] q' divides by simple primes: 0x58dea41af8f56a29ee0b360962c6cebcd498ff746fb7b37c25ea2378ec840d24
[-] q' divides by simple primes: 0x7dd349b763942fe1c6ac7138a1fb2756c4ea77cf8dac131788f1d7dd15be1f76
[-] q' failed Miller Rabin test: 0x417651177bf82edbd7293a4b48a5882d9455fa7a86f5c6ed86dd39982e88a4c1
[-] q' divides by simple primes: 0x70606807b4f3ef7fbb7727b451a38a455c8396cbdaf42b19ea7aa4c80ac7caa6
[-] q' divides by simple primes: 0x53d6ac180ebfa73ed10e3115b71c620791179e3adf40a8adc35ebea38d04d250
[-] q' failed Miller Rabin test: 0x4a7bf597704cb858c10466d72ffb2863959d2b0c98411e740350f1b48913fa29
[-] q' divides by simple primes: 0x64d127bdc8e7cc03ab8eb35c2a4c86c4ad74238ad6930a1d2607a5bcc1375ef0
[-] q' divides by simple primes: 0x791cb5e81609f59dd36646ad65ddccd6a652e5d26099dd3e2f80ae55582e1ffe
[-] q' divides by simple primes: 0x46db25980a06f53856df8902c3d3012f45c7db7757b226194fbeae71ae83d357
[-] q' divides by simple primes: 0x7ff22e794e55ef9733943781afdf0b3e67b92dcf4de2b76c3d35c017db2bd6a8
[-] q' divides by simple primes: 0x5a6de2f020af41cb2b9fb0b5653845b62663f815fced7ae73a2aa7038e7774a7
[-] q' failed Miller Rabin test: 0x556173e0c677a710c191b24fbadba0dd9a0df4f347233deaf3a693253ad9fec7
[-] q' divides by simple primes: 0x434ff440777cc71089182c25dd5c11c25cfa5843bed33b9577e9878ddcf99f18
[-] q' divides by simple primes: 0x465cdb289bbc475ecd9abe68e7488ee8e73525f13e31217f8e39573aadc9474a
[-] q' divides by simple primes: 0x79921ab6450f20b5087cd9b4acc8b209c372a62bbe075c86662c4462b9d3af5d
[-] q' divides by simple primes: 0x4f800b193f8ae56b196e0809b63be3265d3a1cd304814c2c91c2ee9ebd081422
[-] q' divides by simple primes: 0x639e5bd3a0b406693848ecc32c97384f051629f67fd5a2ae8cac6022ec762e1f
[+] p=0xbaf3fb3e56b18b44f16d82d08e28be4f315ecfb6f4c862fd864ae55509f5688b
[+] q=0xd4fbdf88521914d676e42667b75d28cfaa95334206200b4dcff6382a30f8f3a7
```

Таким чином, параметри криптосистеми для абоненту А мають наступний вигляд:

p	0xbaf3fb3e56b18b44f16d82d08e28be4f315ecfb6f4c862fd864ae55509f5688b
q	0xd4fbdf88521914d676e42667b75d28cfaa95334206200b4dcff6382a30f8f3a7
φ	0x9b89fc850b5745908a6dbf9e1a8b9492cd24a32027db285015607e74c73294cf0afe6370978f68bb31f2abd28324a9afde2e70c2c3769569a43d6d938d0cc77c
n	0x9b89fc850b5745908a6dbf9e1a8b9492cd24a32027db285015607e74c73294d09aee3e37405a08d69a44550ac8aa90ceba2273bbbe5f03b4fa7e8b12c7fb23ad
e	0x10001
d	0x47b3c0d98474e2f8d317ecf1f1c2cee72df2e9d0750f2ef25c2873a35a011360aeecbee2b4bbc3c8282a7ad33ce9b5e00148df6aa9b90cfffa5ae71cd23545f1

Параметри криптосистеми для абоненту В (сервер) мають виглядають наступним чином:

e	10001
n	0x910f55be6a1d93e1fbffac02bfd554eae5a1d7f47657aae0f4eb9c035f53a4eb771f50de186daf238324f25ad5768b9f831487f9c1bcc650d8b21690f0640193

3. Далі наведені чисельні значення прикладів ВТ, ШТ та цифрового підпису для А і В

	A	B
ВТ	hello my beautiful world love you all guys	hello my beautiful world love you all guys
ШТ	0b0724bf3b03e732aeffcf134a5d6019691b7efa01a3156612eaefa8fa019268a41ba1d8031666c234df626ebe0dda78d7ad4ab50cd42a4ec0014ae2391d9168	982CFA72802360FC5FF7C812435D028E7B68E7A6F9D3D76F7CBFA4F98571E05CA2AD878726CF3E0056F5559EB3A1A6190CBC6A54A5D4C5F996B2644990067CD3
ЦП	929abb993bf48a97b2067e7eed5395bd6d5d09cb18e0b4883d167cdd547695f3e1161e0325ca768fae096ffb096fd9abe68cac7932f1b94f9ca6ad33f2270776	1B92E2D2D0B9A465102CCC6AC1A071B2EC3BDB31102C8C2AE00938D1EB63DFDE7413ACC674BD765FF951B2FA18481957B6048BC5A20F0906499AA6576AA9848F

4. Алгоритм обміну ключем
    a. A ➜ B

	A	B
e	10001	10001
n	5c311d906ad0bab9867298f7d9ef0ddf2a002e2abce0cb581c0b017ed6b43d8c4a5b212cc7de1b74a2ee54930b6b4836188e332665975c2205914c0fb2c799e5	8ed2007733985cec04e9bbdc709629352f92051dc99f191af759edc4c7228c06bb94d0437e3e607b671a5819b22d4ede3251c1927ccb58ab7442870c0051ebb7
d	2a03ac3083ad6a5b607d5b5f20efc4079f1183f8b02956226a6d4d9a2b68eadf36abceb386a32b5059ef32ef98f17eaf57ec1858d29acaddf7dd306f5be777a5	(unknown)
k	4141424243434444	4141424243434444
s	2e0ab19e1ac35716696746af6e0d9774ff4ea6c86f1618b19deabc5b37267a7907ddecc3ec1a630854843858b49aa0114476743ff6e78e321735a13226c895b3	2e0ab19e1ac35716696746af6e0d9774ff4ea6c86f1618b19deabc5b37267a7907ddecc3ec1a630854843858b49aa0114476743ff6e78e321735a13226c895b3
k_1	088ec96bb00fff52b143066b62b878f5aff531ba7e916fde5845af5fcbe74269fa22cd57ae4402fe8d5b1da97f8d54c7babe532f81cd7743ffaa781931697967	
s_1	3437613da65d6114bacbca116fe9627e74eb03715542ff7eed917a8f8b96adf85da5c8b9df7c6ff4e6029a324c1af25a823b6ae69c95105c79496390c8fa2dc1	

    a. B ➜ A

	A	B
e	10001	10001
n	9b89fc850b5745908a6dbf9e1a8b9492cd24a32027db285015607e74c73294d09aee3e37405a08d69a44550ac8aa90ceba2273bbbe5f03b4fa7e8b12c7fb23ad	910f55be6a1d93e1fbffac02bfd554eae5a1d7f47657aae0f4eb9c035f53a4eb771f50de186daf238324f25ad5768b9f831487f9c1bcc650d8b21690f0640193
d	47b3c0d98474e2f8d317ecf1f1c2cee72df2e9d0750f2ef25c2873a35a011360aeecbee2b4bbc3c8282a7ad33ce9b5e00148df6aa9b90cfffa5ae71cd23545f1	(unknown)
k	c48fc0f0178d0309	c48fc0f0178d0309
s	1b28549cf782f3dd149b7e397c1378fe64644cac4590bb424a282bf7180e25930aade36134e3acee7a057cec3c82b98cd483e6185ee5328992240bd21d811a24	1b28549cf782f3dd149b7e397c1378fe64644cac4590bb424a282bf7180e25930aade36134e3acee7a057cec3c82b98cd483e6185ee5328992240bd21d811a24
k_1		5A8A5538BBCF3214DAD511EC16F523380665A317CB324AA40880CB6CAFA0CFDEE94DA38AE75CF2FD71491CE803040F651181CAAA1EBDCF36E1850471811C0B3E
s_1		7C116380EEB0F0708F76CD8EFE371400AD813AC1AD2ABB55133D638DDE6A4891494511E9FA14D468F8C827273D5B12BEA1C867CC5FD13459C1BC02FCE84A1312

Висновки

Виконання даної лабораторної роботи відкрило нам очі на ефективність RSA як системи криптографічного захисту інформації. Вона[RSA] дозволила нам реалізувати засекречений зв'язок між абонентами A та B, а також дослідити процедуру розсилання ключів. Тест перевірки на простоту на основі тесту Міллера-Рабіна не викликав особливих труднощів(+було дозволено використовувати вбудований генератор випадкових чисел). Генерація ключових пар та реалізація протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу також не опинились доволі важкими. Як висновок можна сказати, що відтепер нам стала цілком розуміла важливість, ефективність та надійність криптосистеми RSA