Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Комп’ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису;
ознайомлення з методами генерації параметрів
для асиметричних криптосистем

Виконав:

студент 3 курсу ФТІ

групи ФБ-83
Самчук Тарас

Перевірив:

Чорний О. М.

Київ 2020

Мета роботи: 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.

Порядок і рекомендації щодо виконання роботи

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 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента A, 1 p і q1 – 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) , (,) 1 n1 e та секретні d і d1 .
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.

Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою http://asymcryptwebservice.appspot.com/?section=rsa. Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Порядок виконання програмного коду:

1. Генерується пара простих чисел та відкритий ключ і секретний ключ.
2. Аліса формує повідомлення з підписом.
3. Боб приймає повідомлення, перевіряє підпис та розшифровує повідомлення.

Згенеровані не прості числа:
0xe3542de27a86b7ca344dc76a7edd838c5b2613fd9dcadb22d01dbef20f2656a9 isn't prime
0x84d7dedfb6e30b4659bef04bc45745f41128b43215b71da943bc7fc01650eb2e isn't prime
0xf87efb31922148329a171bf66428431aeb2fbb0c184a2c30c6a64296f76c2926 isn't prime
0x845d43d4a81ec8c3087001bffe2b42998172d27946620f88db99742d988ba377 isn't prime
0x8e884a10b9102d7836559b1d34848f07bc83a16af55db2a97a18b10bdb695f8b isn't prime
0x988bbd650fe7fbf9b0a5754e82a1e2cf8ab11d7f22ea0ac9e21cde8716b12575 isn't prime
0xf7c2b863c7b4fef6e5fa78ec390defe45b0acb777e611867cbfc2c9524cac689 isn't prime
0xd9cb6b003e39b7b08f13742a528bd1238b0d0edf70b035c28b0f38bd9d66c215 isn't prime
0xdbd5b8ed5f28ef85ddd39e21476f94205b22d042e9b5233522967409bcf7ff86 isn't prime
0xf050390c330d220ab7feedc78a05ae58d4f38208c0556db6c0824b2c9369923a isn't prime
0xcccc5d920c96bcc64dc26289017eb8821f8008d37a1404f712af8fb416117f87 isn't prime
0xb1e01d6a2ddaaaf92b22fbf186429a0c8ca2d625aadc011a80d805eded0c6ee4 isn't prime
0x9f6bfef269def8cfdbee663da235b4835b6e9a487bd67967d2ead0bc2c336a55 isn't prime
0xa8cb72c4265f096a1bccc0fc3f73a17fc494b0a40e5555c0d8a4d5f368097b72 isn't prime
0xe1d677a7b3ecc916d56b51078573ac6aff46037580c54565569687577fd48884 isn't prime
0xbea7b1192fccfa53a0128c02657149f90e1b7b874df709136485115d49fd51c0 isn't prime
0xc0470e936c260be1ca8eed25d4f5145df9066e55dc0f626968f26c5c933fa6d9 isn't prime
0xac6c59240a1cc6214377af10b5b5d4a3231c583cd0af310cdc6f370d348eb0ad isn't prime
0xbed44ad29523fcf40299ff43a25f59a46f33c018387b71d50736c425ca3e63f6 isn't prime
0xdefd8336c0a8da071a8a33900e556a261304ceb5f1b2596e16fa858a3dff961d isn't prime
0xaef5ab2118fd4255858112898412dc7fe41445c284960d9762f5a42069f3b8e2 isn't prime
0xdf8c601b1e08ebaa7971f732f13d4a7b8f57ec8e2b04977ff7bfcca8240d3a06 isn't prime
0xadb175ea1576d6ad9cc0f9b2829be33909e793cecd2d9965cfe29b26381ea98c isn't prime
0xf696f64194ade1867d95fa7f49ae0221bf0f110a09ac2bf6dcd247cd91ba6e95 isn't prime
0x86ec6f3ac2f0175d88f2613b3f87fc217e1cd0e4eee621cd208df6b075bf02f3 isn't prime
0x8d168440a3b9e533df0f36327cfa09040e69b9945dbd4438ff7df9704ce6309a isn't prime
0x837c45b649ec5bfa19eca932f18fd2a19133b7c81637db9ba9e93ecd165332fe isn't prime
0xf1adfd56c2731237fe29564affa898dfd6ab7b173e20de7434e54d14c28f3dfb isn't prime
0x9507cdcc9d11c71d6bd430506b2fc309d093e67b069f81ca90cfe50e48246713 isn't prime
0xe883f3295f3949e28916461a0633d9acb415a32b8a46e47d644fa39ea60d73ab isn't prime
0x8aa2b7b4ecd3415ce82ae669816a8e954a9c5b985068b8e7d309de79f2def022 isn't prime
0xd98a40ecd003aa71036ab5acf56385141233ac452daaef6fbc77cbe62d1231b6 isn't prime
0xd645ca9da81fbe9eba406bbbcbea827163b7bbb19f1e07922d4665fce42778bc isn't prime
0xdb4969f724cda04347cbfa4b5fe733790998de32341d68339a41bf9cf5cde311 isn't prime
0xec1f0ddd18da69cb0ec43ddb79548df427fb31497c9fb8baccbc2c7c774bbafb isn't prime
0xdcaa34c52682c8f58f1516d208e7dc718503245b42a0c0bdbef6e17a07cc9bcb isn't prime
0xac394357e99eeac2dda8dc9515231c2d5134f0d341c6dab969c3fa04416a599f isn't prime
0x8e627fc806e8cd75858d365aabdd6ad6780c6a252d099e7604e7a430371d5216 isn't prime
0xc5cf9187bfaf14b697a9213b3a8cdc6ff11aecb4b6a886670a6853d0a5e49e40 isn't prime
0xa9e4b30db0c117de08dab17677078f410e2fb531913c48618499ef47bbc17164 isn't prime
0xb7c82ad9cf85141f933b1acd37d32af720999928e535bed6261ac6239b297275 isn't prime
0x9081bc746767ec47b8b26634cacea654fd436b1e21613a66267805613aa9c939 isn't prime
0xbd70783aa8c8808ee43026c5a647047ad1c55f41e227679883eb5c0297049095 isn't prime
0xad4405efba5e2fa433692126d4fca0612721092a8851b6a7464d65eb77d2c1bd isn't prime
0xa8cbbfbe2f95e0e0562396a852d691c1f9fbf277d89078b9623af86cc06291e1 isn't prime
0xa66e71ea2d5dc10b27a2cbd2f0b0819f6dd8e3de0f739670f16cd27ca57fae01 isn't prime
0xe720b4ce8bc6b90306613bd9d2443dcf16b10ca2ecea6474994db964160d5849 isn't prime
0xebd74ee6490a71e3e1bc0e1297b570e32a2a79567bdb1f97a50097d8008a7c0e isn't prime
0xcd0efa8f13eb96145c201cd8a7ea8d51d21970daf5deedd6bc9a7237df841470 isn't prime
0x80769a8f6661fd9ef3a69d934eeb4b23e4ec0adeafe45b6fd05afc19a5d7ff3a isn't prime
0xcf0fad3aca3546563f8a3dd6d1bafe5732806c945febab38e2cac68b9ed86ac5 isn't prime
0xce0e6868a41ecdbeeb17a7fcc39af65801d23e0b1b5def9399fbfcd8d84e39a2 isn't prime
0xa4d0ed1271bb88838ce36a8f159e9819eec72953828d258706516efa37a2a41a isn't prime
0xc9b480c38c281b222c07d2f4cbf9d8844693aad91c303141c772228a2e4302f2 isn't prime
0xe637a4d50d0f8657ad2e9a0713e03d280c6f615d2a2ad49d65ce1a9f4056f37a isn't prime
0xd6bdf70d911bdf6aea696e8548f4c370afee48b8c5288d185e50463eddb9153c isn't prime

0xf8bc0f9662fcc1c075899167ea41228c805ab8987531b913ae6d935aed87f964 isn't prime
0xc04f70aadd112b92d4ec4d7d8c67461dd8907c1da9e5bef61f892f29ae6ff7d3 isn't prime
0xd5bf5947730ebac70a5bf1028aff42705986cef86dddbe8db14f43e0396eab81 isn't prime
0x96dd896f5396f023833d008e5e6c5d0b0d9d98f27522455319bbee599ad65366 isn't prime
0x9b2ea203d0b38a1564100af02dcf3e7be100ceba5e7f27ea5cf11a1c7e982b84 isn't prime
0x827eb59f8efd2d92c9442a01c75b231dde74942132c9a24d1d893ed7dd12c3ed isn't prime
0x8b005b864b2e0a7dbb8d2809e9b5984854196b6e3f0861bfdc90f4afd0373064 isn't prime
0xb1ebc0657bd0300e4ca0f28043ecb97eb61fd107d810bf06b675f47b9c2b049a isn't prime
0xbe61330475e50361e79dbc9b298cb7c7b969dd5f578ea392a35f21fe157246e6 isn't prime
0xd6923ef501e440fafbbd96007c126084da9c207125c2d49879822609e9d40e36 isn't prime
0x9ae81db6ffad377580f334ae99c087eee8b3f6f9192d332d1454123f85cc9ea4 isn't prime
0xcc38fef06d54bf5a3a2f629acd7992fd0b03df3f57b37b5cb8d78bdd87044b42 isn't prime
0xb85ce44a04ebd77d9495ffc3c34db0592c79133a1ec88bc6aba869a7f0325afb isn't prime
0x932a7005b95038b1539b382631d392621e8329f6313f72a417e2e5177b678d5a isn't prime
0xd54b0a2912c2cf7ebf5c61937e29cfbb236c3a8cd7337d7a53fe1c3d20dc7533 isn't prime
0xd0aafef7c3dff079b2fc6ea60338775ffdcd86d894cd178b0e73c46c4844143e isn't prime
0x94953de0574acdbf33ba1c3221ecfd9dd332393145b5b6e9b57cc038b0ae05b4 isn't prime
0x87463479dc1d37de567fc8c403c4a5aac65c20507d138d6432d51c9fcba18a2a isn't prime
0xcd447adef4a8244bf59fbdb8643af9b9303b7566c3b4d503070cf1369effd727 isn't prime
0xf078d7693bb3dbcdb59005c79d82388029c9a9bc0936469787b1daf2d1ee1a25 isn't prime
0xf0f09715632f36015473e261cd1228154aee414fdbc92b06b2153971c59c76ff isn't prime
0x8d2ed633e43eece3408453b29e9e20d4242e07ad277a425140f66b6783ecbb60 isn't prime
0xcda5989366310d4fc8251f933e75862b25d5516d3fc765eac5376476b9b2177d isn't prime
0xd7fb8de50e65808c723a37ca716a26cb32ea48306df38fe6022f72a15bbdd525 isn't prime
0xfd0db89ce2a4750f1cb79a28575f042ebc25e646fd1bcf89cafeadddc5a0a1e4 isn't prime
0xdbbc39f5aeec2c77de9b70a8cc15a0b60e81adfcc17e067d3babe67f32953459 isn't prime
0xff03fdea1a8fd79ebd5660a032010d40a589f6ddf975577c9b0fd76f219c453f isn't prime
0xaddcfb28157db21bdfcd631fe4d767677b6afcb69d5f9311b0366c762daea6c4 isn't prime
0x851a3226f431864e49bb5eb9ffe056b7bbfbb72d43bbf817a6be15a33d8715d3 isn't prime
0xc7969087c21f553d7f9fbcf97887d2e2192d82804c764003fc180db5acd4e499 isn't prime
0xe4aaa14f0e7fe54c4248cb07b3e122a345dfb9d3270ca5ce879dd87aa5bc107b isn't prime
0xdbb81908db83da6e0ad2f86b71b51ba95433f3cd7954fb760f16bdb2abcfa912 isn't prime
0x9586e9435ff29fad498935b445e254956d604aa517c06f94e297c2b41e673fa7 isn't prime
0xf4e4b1cbf77ed5a86990029d52a9cfbd3899c5a35f8b131bf6d9de32076fb1f9 isn't prime
0xa389092503cc0488f662592c440a0eb5623c1c158dad05922171e33c9057ceef isn't prime
0xb04c93d1885e203fc36d204d43fccda20660c5ba9cb0ece3e073221b0ecad432 isn't prime
0xe3f619dcb4e7c5f69c13e0880847e7a7dbef32ffcc93672e20728f543492b5f8 isn't prime
0x867eac1c93cc05fa8bb89e40a5c0a676c19d325f8a89e160ca9207c4a0663edd isn't prime
0x87b74df5e6eceed2789d2bb10756b8e5415ac4fb402d3ea969ba3a7a4f7eac96 isn't prime
0x9384e2f90233fc5eac81318b4b626c90102fd8f2f8a0bdf0ef0beead982979a6 isn't prime
0xed7f8b9d4032e41b585133980c9ac71df4f7b5e572322042f49002e0ccfdabd4 isn't prime
0x9ab692f39996612ac6778d12a59f44b4f83bb754cc9eb5de148d1d195da53a09 isn't prime
0xf7802c642b098ce35a1e4ec65c19cae75f1911f12a1b7d43e832fc98f893b833 isn't prime
0xbc871bea4ecee33f1522fb47783d7b588cad6ed1542a1eafae7aaa9beff7f830 isn't prime
0xa3ff2207678dfc36bbc76db11d1608e31bd9237764bd4f00a01d1e54cec582f3 isn't prime
0x80d5e0362504edbc3b3a1fb59a3bc4b7cabd467df4571e0744a8371b47aeefe7 isn't prime
0xad4bf699921f420deae31f9a0df08e4406139cbd47de33c90ec07be86da9738d isn't prime
0x9d1dd666f942a588ae18ce15e2c97130bca2338d0bb6eac0d338f3084e39534e isn't prime
0xd36a443b34eb465a5283f8ddaa7f18ea85c0fbf8b50e8d62e2f1770e7e96e78f isn't prime
0x9dc4d61ed49a350236a6011d5a04aae6c3cc2df8e20e2635bae6aa9c21ed7250 isn't prime
0xb221225d9c5301eb87aeb4cff1c78d1b6135b18022721bf2622893795affe781 isn't prime
0xdc962455a9506f39a7c8e1d0c8f425dc6df62ab71d51c8469596b130740d3e55 isn't prime
0xceee13071a1d1dacb9e87c6839e905331fcee42b27d330e0fd21b2edd75a5bc5 isn't prime
0xd92d28386419e9072eb2b1d8c70ba871b0e2f66953ae2f66df56f715279e6a2f isn't prime
0xccf16c97453539b9c92b3354602994a0f131cb0f3377aa9f5759ce8180189e13 isn't prime
0xe6e5487542c150e7351987b7029c32a7585a7c23f69efd58ca54bd69665b77b5 isn't prime
0xeac217f3e95f142ec945f93315571eb6e1008a1d565b0c21fe0c8bc5463f0946 isn't prime

0xb20fa946d32a3bb9ace121857c03c1e3d145d1c3c5cd1e5698edc820e3986e83 isn't prime
0xba4ac88bdf50aba630e1e9eb2aedcc947a1a9781f774d8cbffdc2d93cdee5155 isn't prime
0x83c696d2a7768bb294e74854a228ff1094354c1fa83f0b41a9e0a0927e854e5d isn't prime
0xdffa6beb0192c44c7961d177963f6498c15e10bb23185e83caea73f765b563f1 isn't prime
0x9d579af67d018505e7cb0ae0462bb0b4c3ce5053db21cb485ffd7ec769889e9a isn't prime
0x9eb2410b0b8852376755f6efc33da36aae51df57d64e7113e0f9eb36534619a3 isn't prime
0xa9b164eda9c466ccca11e409ffc66fb4cc3921da9bc06e6c9ff09d5eab045219 isn't prime
0xab19ad7154f8e0e427032475d84a97e2078f5de43b0b167b93c23e11fac8d329 isn't prime
0xc2a29a10f10685607ec86f83c93adbe4cf5cb991bcb8a45b0081766d74c2c6ff isn't prime
0xffc15a2816411cd7759a5a002d0caa0e7ab9ab5e264f7b531fdc4328c15e234a isn't prime
0xeb344b02534ed549d39423dd5beaf1a99d2f6ec3baea145b57e823a9d236c1d0 isn't prime
0x92d40698af32da89dd3a6fa5806988d18c31b376fed03cdb4a327ee918f45584 isn't prime
0xf7a72be46fbd3ee8cb1b9c193f8d11371acc656c04ae5321e51da3549c7853c4 isn't prime
0xcc231c632ad74d5a519491606a756bae5c0c87814891fce096c0dd00c7e42697 isn't prime
0x8f0ac6e00a9f2d10d2d95d7f373c198dc97557dabbe296f647d891b9df6b90d7 isn't prime
0xdfe92c606aa53c2e6c3d239833c981aad3efb6d010cfdaa0fdb8aae5ac15f079 isn't prime
0xd5f97d024d3bea7748f591e0965026a5de47870ea13a9798357e0271591a1a94 isn't prime
0xbc1ce624cc416767f9d1477b2c431ab40f3fb86d0b4714f5f42c50971e7e8b56 isn't prime
0xf7575e5aad307fc46014bfa20ffb29ee862657b82b348fbd636a1fffff9d8ba5 isn't prime
0xd52533a4855525a52f408f031caa230db11bf11cb4e3b706054698cb4707def8 isn't prime
0xed42b6a68baec574c50932916e65be86efe265023d8de04c0f6b338d435f9e33 isn't prime
0xdfe3df5f21a578d65c094ebb65eee49ac641b0cf70c72721b3ecc3ff1b05fcf1 isn't prime
0xae22d9cfff32a6367b8446e10db9d691f6b0bb0a390e9625d10f27c27f8e9cba isn't prime
0xde68d9c340a14b958aa4c355dfd82525ab08b903f9affdc8b5547051a1ac9afb isn't prime
0xb6daa444229544685a2ba90ef8b228c5029187a5e8207993884a4e435aa4b7aa isn't prime
0xfc63d93aa83ae3b0b699c2f30c31a8ad782233394895f16d2b5185805c434176 isn't prime
0xe53abc042a779f969d572aef6cdec2b74f38d75f287dc512502734f3df4c6620 isn't prime
0xf6448688baa540454c50e8e8ffb05630460cbc2704c4db0713c43491d5051157 isn't prime
0xcf88b5ec4bc6c0d8ef082883a9737fb9f0d7b78a7b2d8f25674d7aca110a7639 isn't prime
0x9b5eb5c0c7db207dc562f6fdfca0971d81592dbbfcceab83d0ab2ec1910e9254 isn't prime
0xe55e3f9e99882eab31e9a432e3eecf13713201be0af1cc7a2c08e7d3086d84e8 isn't prime
0xfac62fdfafaa7b28bdab5f6e45d0ed57873d492351dde5d5086f9a2f1902721a isn't prime
0xb24ba4277ee8351616cdd377d7f73e0898545bbe2a153b0fd7512ca7b083765d isn't prime
0xced2841f21ddaa3da7280ae9c0566ee02cb7742bc73a932b2c715b4d40080401 isn't prime
0xc001c997dc3e588312d4ec48bd877872923bc6b5ba4058793c2acca42540527a isn't prime
0xbbbdaf397f522091af121dedd502182171ed7320c298622b483fc7efa088c47f isn't prime
0xe258a84fc0f520191a6fd81d471c15708909c37c073f8367de2ee682c914873a isn't prime
0xc513681cfb6bc4edbc3e7b37cd66f2c81598a24d1eabdd2aa2071a1f240169e6 isn't prime
0xebf280f768b5ec478b42e31893d0d1ff30ca45f289c13ca3342a97e5ed0fb7e1 isn't prime
0x9e361107d704c795a35b04e905bdd83cf873639ce1e6667861c82667720d458b isn't prime
0xc8e90bad799bf947ad9f0bdde0f72c5c76d1c00761323bab44cbfcabd796feb4 isn't prime
0x8bb8891e1bbeaa628fab12f6d45fe3999fc04a7cfdee2aefc2bc305827f786c1 isn't prime
0xb862c7bd4a82af75cb27b8982fa76385752ba8c755bc80945c4459436a02e210 isn't prime
0xc40de065b6627ba74877b65a0193f0afbe623d9f6596b8bb645784531c63508e isn't prime
0x9ec208edb381c4b2b1d39d4c1af79b7639058a83f3e5099b62f8101b08f6a6cb isn't prime
0xb28c00a5a93d1a958bc93db26d44eec878ba467c42cf2811e21a65b9f891511d isn't prime
0x887c173bb06168643a0ba4047c8dad99505c23e945e77826219e380c7578cb64 isn't prime
0x8bac56aa5ab3c8f8ee928c21fbe48ed35d81b5ffcd081509eab04e87da1d6b56 isn't prime
0xea7f37b70e284c928bbb84df3f67f9b7c4aa6dddb86e6d75f505eded255f664e isn't prime
0xcb34813d6f665acbfedbb4ed419dd77b3a240e06166e5264bfa5cd18b3659571 isn't prime
0xdaa5c87be5e1432674baa47e82cf77c62ab172b8a647e7479c2a2ca6c0c09dfb isn't prime
0xca8c17b5606498c1dc562e673ec88b49d5ac4c8e4b02df45f4591c4272c6a09e isn't prime
0x947103899130df1d0bfb8875cb94f90ba9b8ec5b35134bd89d1ff528eb206ef0 isn't prime
0x8cbd73aaa8bba75b89614dff56eb7b47f21f50483be4823e20b165e0b907ba71 isn't prime
0xe9d81c1b1204a7ff2e3f77755dd4c05a2e75bc64f7cfcc50950a2e0727c919ef isn't prime
0xc97171dfeb038c041723f704597276dfc5ae90c4a629f88d2f0f82aad494f821 isn't prime
0x9157256624c1bdbd6a42ce61051ba65357f2a8a1a7413072cb83d941f4d65f39 isn't prime

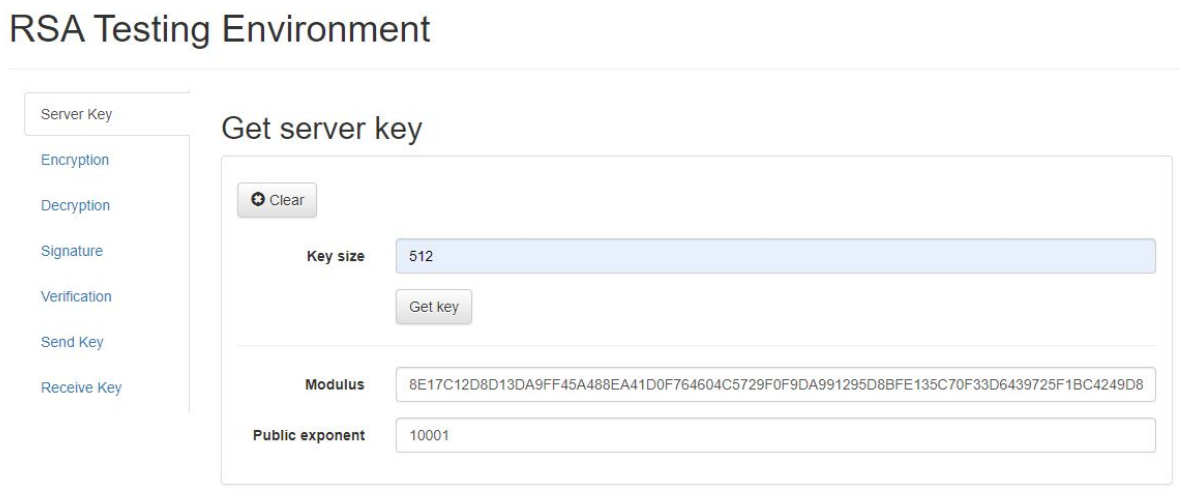
0xf288072af6d8171844be3891fc26d221a67d3c13d7d3081bfb08a45527f96c59 isn't prime
0xc332cdec78ccb186ddd4bbf2fa31b6c123856eaa8652443df39eb52409a9bc43 isn't prime
0xf40b4809d61290617c8f4acffaf55f23351f04653695912a40703a4d174b2a50 isn't prime
0xf97bad1e143453244a135bd406b4ae03287c362a490af3a769adc3329d676a1f isn't prime
0xc0c9eaac43467bb166e803a6d19cca49d688450d0dd25c309321b495268628f7 isn't prime
0x97c24b193ace8719c3eafc73861f5e1e211a256c91d49127541b5a31c641aaa8 isn't prime
0xe8562671dfbfa3c2add4d0a93378707750b250ba00cd51dddbb1a158a6cdfc78 isn't prime
0xe436ad07f551f400ed41833f38ea625eeeb105382465c1c5308fec9355c17af7 isn't prime
0xc2905838705948e58c5de4348b4581c70c59d766898f70f4a9624f2b24c7e117 isn't prime
0xaf084b8bb0453ecb3f40bd09994cee2c2ad1fdf325305a2e227ddb0b7025ee03 isn't prime
0xb38f42ff5356f31f1c117797c7ff36b9266feaecc298fc3f03c91e7d4d36a7d4 isn't prime
0xbfe42aaf06cd4cb1bb337078ff5bd85625f33fd41b64fe63d4d2a719a5daf7f4 isn't prime
0xc47a4104827ecbb2ade7ccd81a444d2e4115e6a4012f542f6c5e4fea7ea4468c isn't prime
0xb9f74ba5f89fec42512ec1dc9c4ba52b2d635c497b4553cc358e5deab93269e3 isn't prime
0xb7fa5750791ebfdefc11b10740c96bbad016281d7f66c17f720403546f9a86a8 isn't prime
0x9dd7267b3473781c8d4bf88632dccdcd9012d26c9dce7e101add4b3a88f1f287 isn't prime
0xd84840d22359e07a1e5607c03c2fcf084d3cbcb8829871bf7b5a67f746c641bb isn't prime
0xb337a806aedf391154a620aa03979293c066219e0f5bba17f6f7c650c7c4a147 isn't prime
0xbfa88dfc37d3ccc0fb407404a393a69ccda8b98d384b359b0684a0d238cf9afb isn't prime
0xc464f958d7b80708e5a3a741d9ff6206a1f90adc67d81c3a66bf3a8f2a033a35 isn't prime
0xce6a5392fd9342c40769640fc9eda8facb7516d97008211f2e648e26a2ac6b22 isn't prime
0xaf3b96507c3fb9f2fcdc7a359ee21c141851e1e5799ba8fecddaf2ee99de7696 isn't prime
0xa5080dfa29a3ffd33047be1330ef469033d122b6a6d4078ee5e7629cced5ac53 isn't prime
0xd8be096a70560b6d5c54840c01fcc09c6bc4ba52cc6a4a1965e5dabfc44fdb45 isn't prime
0xc5b276411d1a4148d3a788fb12f7ed04655ee264502991f0fedaee6070be6765 isn't prime
0xa76d8a7426127546267a09f0db78e28038bffcf6a0ae92998fc2fd60d5550eb0 isn't prime
0xa88a2c140388001fb2a71dff5ea9b08a76cdca965c2c1dbea379a8817b844a13 isn't prime
0xe96bd9f35195374f1310eec8588836caafa15047bcbaf6b5e2e95b87693ff232 isn't prime
0xea62a15b596f2e0a7f46095c52c19d6366ed04317898a05b02e4be197a226fb8 isn't prime
0x8e8447af7e0766a2b2b9485762882056a07fe630ef2e503b0a1f2258d1560df7 isn't prime
0x9dd6ddefc876fbd5b326ecacce1917cbf7ed4688ddcc4725f60058c319e1aef8 isn't prime
0x90161e137950b2b93c2631b8b3ce8b4f6179a704019a70faf8d3e18d190f1da1 isn't prime
0xbb82386736d1b6fe14019354220727259369a3dced4e3162c983cbe29cf873b isn't prime
0xba131dcd211bef152dd6c27fe9e4a56c26837428c5bae06a1ae597297b656dc8 isn't prime

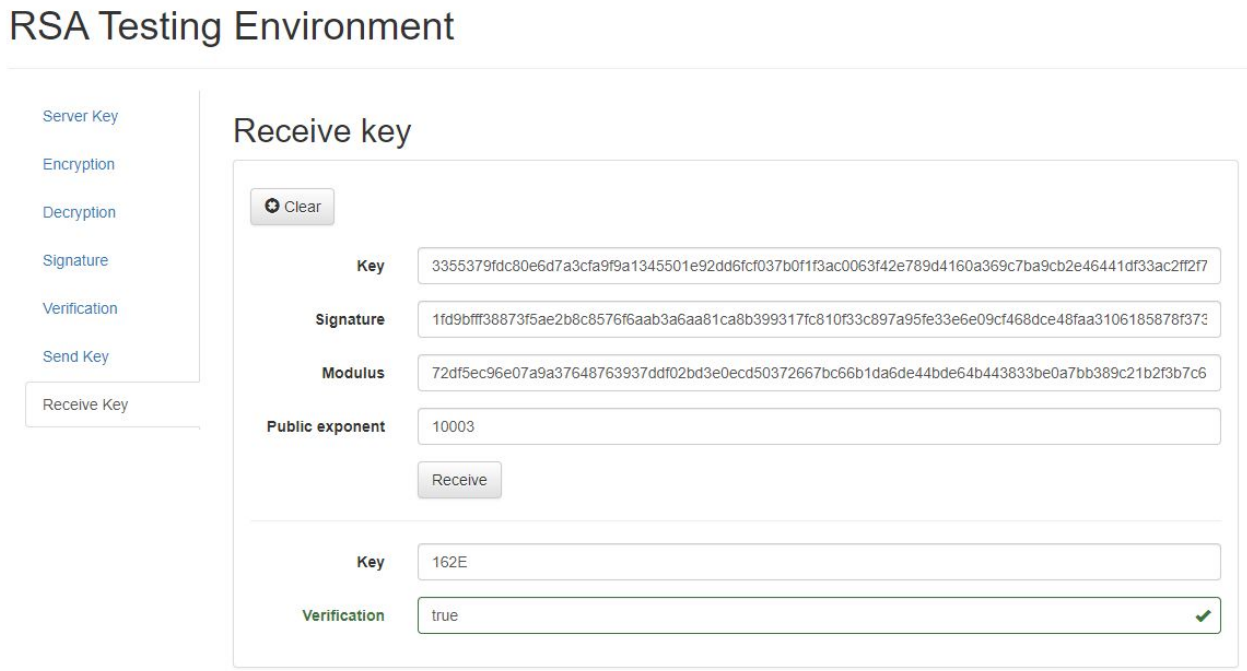
text = 5678
p1 = 382857612649569050849894147158763746413577185135134437097532290602538922980356 33.
q1 = 370399400734005646895211986870753053760716693032555233630134272676489043640358 67.
n1 =
14181023029185243633497370907041506635584716400217049872782575499515054226566876529524345023288461861808381153326300652766632567234968357466904482362560560488 11
epsi = 65537
d1 =
93282253198677976263800854449022590454255935427828100159552135402001005189022691718401005079277411396773406397520113161566816022155085039091308615858880440609

p = 57013925710858322851831249022746009117523640078483411322617660716669549786409587.
q = 55689830118419869009305145014097336662138482431590662009595383233239501506823277.
n =
31750958372219107680896947630004635740825281179035648941496983755971343824148755711492121688155594979373611723670396943364979871260573787102794023588439475565 99
d =
32915268256472119278659615400610242407900652074359983222480796045155988231110630883073701367878701257039373082762630900416939349387121672623402083947333 93

cyfr_text =
106138564697507613078952840226526637685847400706729850249539155227365317987553492153214965021192488940907042024170602703375524643571640773590467215352871323075
sign_text =
898071950031733838543173952416311155973520769734247569832471043553857463220187012862001742301448965575186397861740196164081380407988579699508131642948762879 76

Робота з сайтом





Висновок: під час виконання лабораторної роботи №4 я ознайомився з асиметричною криптосистемою RSA, генерацією ключів для криптосистеми, а також генерацією простих чисел. У ході роботи були реалізовані функції GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().