Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського» Фізико-технічний інститут

Лабораторна робота №4

З предмету «Криптографія»

На тему: «Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем»

Виконали:

Студенти групи ФБ-83
Жоглик О.

Купрієнко А.

Перевірив:

Чорний О.М

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 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 А, 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 А 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 А и B, перевірити правильність розшифрування. Скласти для А 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.

Хід роботи

```
('0xec68df3cf42e037b4ac424f508a0baafceddb3b2768be6caf3fd98472bbf0bc5', 'is
not prime because can be divided by', 7)
('0x92e5c04d8787f87dffc6a75d6cabbbbb7cda56e15d45dfe623c83dfcb46a5434',
'is not prime because can be divided by', 2)
('0xa9f86a319dcce96a55b94e3b4db51fe578509a82d07f59fe9f74fb53dc3fa072', 'is
not prime because can be divided by', 2)
('0xa672d439b5431b88182d2638ad05afe7db17738fca9ae54482bb145d2a24ecd7',
'is not prime because can be divided by', 3)
('0xfab1a86f73f7fea3f2251d680e6e5a97e6d2b41b1a9424fc73e835eeec1b7f12', 'is
not prime because can be divided by', 2)
('0xb82224c5667a0cd6fc5af06cdf23c65d62d0b005490e38cc94bad4fec0b14f6e',
'is not prime because can be divided by', 2)
('0xd2c6cae5000d7ecced650e002099291f13f6ec1f7efba13044e300ec88ccef4a', 'is
not prime because can be divided by', 2)
('0xcf9402c6fdb81e23113ad77d152369fade11bc93b12f0cb0cfb9c8da4bf78b25',
'is not prime because is not pseudo prime')
('0xc0ae86a61b30b59eebcede99ce57e247201e87d6d3c3be2cfb8b4e5848db7135',
'is not prime because can be divided by', 5)
('0xd4fb698d562a916ce6d48f2fce479ecd29eb645a96bf7c30c5354e7d0bca9204',
'is not prime because can be divided by', 2)
('0x96df6558ef1521f4b66a2306393b6bc12fb6a17e7c61de229db50d8183cdf8c8',
'is not prime because can be divided by', 2)
('0xb56d528b526afca214d162065719705e7fa7162c626329c633dd39df42c9bda5',
'is not prime because is not pseudo prime')
('0xd0de60762bbd79193d92df057ef53f31c1ffa14a77353c30ac98f279b5fdd755',
'is not prime because is not pseudo prime')
('0xe394a0735b125f4ecbec204ac5310775617b96bc882c4dd439cab9a493e048e1',
'is not prime because can be divided by', 5)
('0x950b1aad52a40f567815c5e34d4e4c85ef7f5d390c357e219ac29f7ae6bedc4e',
'is not prime because can be divided by', 2)
('0x986029bf0d5587c2f247c83b24955acf54d39516972431d23931919a7983fd1e',
'is not prime because can be divided by', 2)
('0xdfab7ec525e79660fcf25cfdf77647ab132cc2e890630a8f4c7527ecf026509e', 'is
not prime because can be divided by', 2)
('0xa92e36c31fbaab4ee0c51034d44097ded13bc60cae6e449bc0214890b109b3cc',
'is not prime because can be divided by', 2)
('0xb93bd26335215deaafbd1b27776ba93a96aac02cacb25f88dbe2640273b73b70',
'is not prime because can be divided by', 2)
('0xf243440d81136df59d61de4f6f25ab90f92f17067df5a5dcd5771e51c42ad8b3',
'is not prime because can be divided by', 7)
```

```
('0xcc299890e676a87d2ad07aebc56175dd3c1e3878641096710507950e09a56985a',
'is not prime because can be divided by', 2)
('0xcfa6d5e589940230b28cf17d826fdbbca9bb97eab043afb8c271a6353319bfd8',
'is not prime because can be divided by', 2)
('0xdedcc654e28ed94b7e2e629b260cfb7ceff1a430f0920fd41c6cbc32f3ca405e', 'is
not prime because can be divided by', 2)
('0x8bdfecf9dbbed2782095b5229ead1e47920b72dbac167036bdc4c7badd0157b4',
'is not prime because can be divided by', 2)
('0xaea86663c1863e10bfb8cbbceae1066b5f86c43a77c4b282d94bf1657cc4070f',
'is not prime because can be divided by', 3)
('0xf4bf1f9552e37f74287159293a7888fd3282a1506c0cd59c1a2a58301c66a348',
'is not prime because can be divided by', 2)
('0x9eeb407176683e7eb3454e38673f12e599184add41d7543d716c69446362e20b',
'is not prime because can be divided by', 5)
('0x965e3289af6ddb6be60a93610f470e121fc89d06ed2cbf0288fc784368c46ec3',
'is not prime because is not pseudo prime')
('0xc37672c702e0ef92dd41b14735c1d2e969d90a0f46eb5e40bf7be3582fe3c2dc',
'is not prime because can be divided by', 2)
('0xc0bb3632dd26b5c9c6a0e96dffc3f0340af62d1fa1bb0f1592c008961b4b5653',
'is not prime because is not pseudo prime')
('0x9c0d2906a8a59b049737ab8ab93d793d0a736f91d61455874f48827c3457c501',
'is not prime because can be divided by', 3)
('0x860623ab77936156e6d56e495a3f830b3ddd3be9b3bf90c6d6b71d9a9b89b884',
'is not prime because can be divided by', 2)
('0xa84d8eea3deffdd4b799f0e327316f197c29de97dd7a4ee1d36c6303fb69c83c',
'is not prime because can be divided by', 2)
('0xe9ff3f1a8280a296ae17f8b7fffa0c1fab325a5ed393c7dfa3a7c3e3457a152b', 'is
not prime because can be divided by', 3)
('0xb60dc853f29c5a0efc856f1af7f76804c67d2ccf74cd339128d2914f35287ddc', 'is
not prime because can be divided by', 2)
('0xda142295d10437e33008f5963e2af56ad0560e5a287337806a1a143606a59d15',
'is not prime because is not pseudo prime')
('0xfa7fc256710d3fb4fada8160520de0d0a1d6429f2b288d2e327090cddcbef0d8',
'is not prime because can be divided by', 2)
('0xbad1b07cf6ae4dd5784a01cc042c8e52c559af05f963bc3f0016967204ed38ed',
'is not prime because is not pseudo prime')
('0xbb48757e88213cc46abeeb37c6cd917caf15e734aca54490fd23b0cc39f66136',
'is not prime because can be divided by', 2)
('0xbab2c0267281034385a8bb013200cf640dcf6786db3f9871b3c49d8d55be603d',
'is not prime because is not pseudo prime')
('0x819eb9b641a8e1d74ef41693f20606e7dd48be5cc08c1b6a12df73937d00af62',
'is not prime because can be divided by', 2)
('0x9f3ee6de89624967254d440d673e8213d3a4e96a1577c5bd46af85805ce96128',
'is not prime because can be divided by', 2)
```

```
('0x8e10e20a0474d58555668f2393651ed959e73e5562b73ee9688b2764053c3e3d',
'is not prime because can be divided by', 3)
('0xa3b8ea0d311d2d899a198e796b22acab0d30e63ed88868604fcf4d2b7619d99d',
'is not prime because is not pseudo prime')
('0xc7bba062f820995bd22fa8596a5f49182ee103feefbd95aee2197d4f09a1f106', 'is
not prime because can be divided by', 2)
('0xf74fb91c5df51828575b9fb0e6b2c6679279005795df2fc1a7b11823b5a27f10',
'is not prime because can be divided by', 2)
('0xb7165b1adeaf0e9a84d999dcbe5bb55564720a82c6b1f0d0bb18746d380758dd',
'is not prime because is not pseudo prime')
('0xc09faa4695a1ecb6bdfcbba6f32411354be77efef05a2cffa73e01294b280c65', 'is
not prime because can be divided by', 7)
('0x92208d4adc33dbb05de379b871e95822ea9a150c4a70ba037a59844cf80e2f30',
'is not prime because can be divided by', 2)
('0xfcee8839e051f5ef4097814aaa8cd7dd188f4a542444975bfed9f46a398e2b7d', 'is
not prime because can be divided by', 5)
('0xc45e7d1503bcd307876ec146423726c8d759d5a92c2ae924df3b9f27d3079e08',
'is not prime because can be divided by', 2)
('0xeec9490e0e08644e6f0e63479c84a97c63706ea987ae647f9a5360fcb1764f70',
'is not prime because can be divided by', 2)
('0x9df9ae3d125ce4cafbfdb4ec618f7a7e568d745cdedaf0ad8b0c8f47e2eb9cfd', 'is
not prime because can be divided by', 3)
('0x84eecf3cf5bc2fac8d7c55ef34871d6574a8584bd91793cc09ca04dd3e0f9b4b', 'is
not prime because is not pseudo prime')
('0x912baa1344257f2e5f4ded8377fd8baf73f5262a6d9d4979063411a5543c3cff', 'is
not prime because can be divided by', 3)
('0xad95c00eaf3857093b2b1f41ed91777f3ec8ac34767743111be87a2cb1083d5e',
'is not prime because can be divided by', 2)
('0xf39073f5047d137d39d48f23c416bb49a4e5ee64e7984e607e6d6ead8a3dcf54',
'is not prime because can be divided by', 2)
('0xd99aef50436b36364b7e99ea7fcf647ac1656be0bfdc3dc52050865bf6087004',
'is not prime because can be divided by', 2)
('0xba6d05277e4c2cce333303f57a5d35473b378c7d2ea9b8638e85ca280f3f30ab',
'is not prime because can be divided by', 3)
('0xd95d8a6d6a682f68d9bc9fe18a15045390cd6ab349225143cf115bfc01a8d543',
'is not prime because can be divided by', 3)
('0xdc91c337d7ff799eb30a05f2a52a3a6d3ba1b149e82dfa58ad679621a9d35b9b',
'is not prime because can be divided by', 3)
('0x9fa6c25b5c1becfcabbe89c26bc45f4737cac008f8ee8ac7d71116364e76d0c8', 'is
not prime because can be divided by', 2)
('0xefb8f8a28f18ff23b7258f7737536df15a62fccbdb9567b1cd42fb1d295c957a', 'is
not prime because can be divided by', 2)
('0xf562f3f40dd6eb11ba1dbf8a884b76414fa821ed6e26de3ab17a7dcb36336733',
'is not prime because is not pseudo prime')
```

```
('0x849fd5ee09de1648f9454167348fc34683c760dfc0faa6e324fc49895fb9a50f', 'is
not prime because can be divided by', 3)
('0xbcacc181886f6e22fc318bc781abd81b3679fa4f0e8130aa847c162e649fe7a2', 'is
not prime because can be divided by', 2)
('0x8cbf109148c70476112964a8aebe3050464c150185488c5f6e99a4c446c8e1a3',
'is not prime because is not pseudo prime')
('0xa0cbdf4ba2c5e19f22b3031c56b03fd5b288c85531f8f8e7d5d1fa53a0bbb063',
'is not prime because can be divided by', 3)
('0xe4c30ec2df9a4b72e14247a22aa81c018fca0b366404388b1071cd4bb5e7096d',
'is not prime because can be divided by', 7)
('0xd8347ea857221b9e293d70e46da2680b303364bfe8667d857099a6c8030d05f1',
'is not prime because is not pseudo prime')
('0xb6cf262ceeda77d3e2c5322b7655f7e291cef3c8447a844519bacb52ff31c78b', 'is
not prime because is not pseudo prime')
('0x80013d330d6aaf173b0b02a9e8f1ba4047d27f47edadd0c00e8a8e226674af4b',
'is not prime because is not pseudo prime')
('0xcceaa9b2abefdd511f679dbf5d00ff64a90b288c95155df945043d6239932282',
'is not prime because can be divided by', 2)
('0xf10cef9b79d8b534360311ccc75d052b8a2c6972714ed019714448ff1f8947d4',
'is not prime because can be divided by', 2)
('0xeef98b495422793f81837a5a75b491a08df59258d91b69bb5114d3847fb3206c',
'is not prime because can be divided by', 2)
('0xcc340b732b65bb644be3cebf23b547fdbaa9d6d113e822049929c7a9efc64336',
'is not prime because can be divided by', 2)
('0xfc817e7e3571ff45df8ae4d8639f0b73cba750c82949383d04da9c8323b0a453',
'is not prime because can be divided by', 5)
('0xc5e350f2c5d4a7711cac56e71a7f99fc4de81e007307a7f7bca85bba43d2eb98',
'is not prime because can be divided by', 2)
('0xbfde063884a284323b603f49b5b906edeb2f92fec24d35c15e5caa26dca40924',
'is not prime because can be divided by', 2)
('0xa7c8cc8703aede996f8dd62c426b81f8132b264438a0578f053de75892d01ae5',
'is not prime because is not pseudo prime')
('0xce06479a29511525bbe23963d4d735af4bba93cd77ba74767b333b476df0f31b',
'is not prime because is not pseudo prime')
('0xbbb9189d13bbbf90b69c32f96fe9a73594cc4c1eac2860e20902f56d74df83a8',
'is not prime because can be divided by', 2)
('0xea4c70559aad1d8310044bbeb4c59842f707d094235f14f3dca61e67c617cce0',
'is not prime because can be divided by', 2)
('0xfde1d18743fd68960473e324d76cb77619262de6a888d43da7d475d19cf620a3',
'is not prime because can be divided by', 7)
('0xf1e8d6dbb0dd8fdb360de8cc6c6c19a9d92d80d478c2acba596928934498c293',
'is not prime because can be divided by', 3)
('0xc1c098df471824193b8e20aa79d47020f747fdc80fe0ae4952a748a896f83b81',
'is not prime because can be divided by', 3)
```

```
('0xd104c6ff4f23b688bf3deacc0294ab9e5f28633d9bd5bd4e484b5ef9bfc1d1b2', 'is
not prime because can be divided by', 2)
('0xec23071e87f40a71666230f3fe124d85b5003e2bb839e0f0472ec0fdf824f06a', 'is
not prime because can be divided by', 2)
('0xdd8a54fae5c37254861eeca8db538a323484ab8dabb5c168985d9756a6b0ae08',
'is not prime because can be divided by', 2)
('0xd900673529a5fda6da1e3ac995f305b713bf81fbd8619efeb27ec90cd5440ea6',
'is not prime because can be divided by', 2)
('0xeafcdeb6293e6e96deff4bf71909f23beccc5d0f99e16a82e19a76bacb216c5a', 'is
not prime because can be divided by', 2)
('0xea3e05729e026596ed3ed0b91e0aa0fbbc5841bddee69c1551e882884fd7dd7e',
'is not prime because can be divided by', 2)
('0x9819e08217983ce865420bce8da148ae18038d4ba59b62701747a16b1e75b4b0',
'is not prime because can be divided by', 2)
('0x8dd5f070b2bc68a43fb99cee24a64e33598b5f1f45deb3b95e13747ef5a728bb',
'is not prime because is not pseudo prime')
('0x8935ebb959f4a6bae0a0a2e80fb3ca9a39a427a97cbe67f262ac7721dd7945d6',
'is not prime because can be divided by', 2)
('0xa8f79bdf37a4d8e2da49e6c5032198b62712c07641224259a8cf413b412bd7c7',
'is not prime because can be divided by', 11)
('0xdd2528121ea62bb448c44bf03a8c3e44387d230ed615d3e316d233dc069f8d1e',
'is not prime because can be divided by', 2)
('0xa7b3eddff02fb4898b42b8b59cc22d4d73f56446c9d854f5fb34e4dbb1f92654',
'is not prime because can be divided by', 2)
('0xf2ccd707c5b725fb85061530dbfd656770daf29212f4ccd6e541b4e4d6d01340',
'is not prime because can be divided by', 2)
('0x876a79cb53ac18b6dc054ea827ee6453f814697c16839ccf8852b6f2cec9c19a',
'is not prime because can be divided by', 2)
('0xfe1069ca4b2260a5fc038cac0fae7048d3780cbcaf6b978ed6bdc5d4e0df899e', 'is
not prime because can be divided by', 2)
('0xa03574a09d22dcaad8bac1e88209fecee154e099e0f939a721bfca1d0b88ac56',
'is not prime because can be divided by', 2)
('0x8def8cb58e77ec8f603ba86f57c00b4d6f5774f62a39eb9d7f98f18cf911291a', 'is
not prime because can be divided by', 2)
('0xbcc5ea78010c679d2ae4303363d11ca61c2ccb85b96b95d07b0e6a45a007532b',
'is not prime because can be divided by', 5)
('0x86ddb01f656268c618a7e856bde6d41b54e66756011ba71c0a8c51e1e538e220',
'is not prime because can be divided by', 2)
('0xdb9fc2d72a51ebd394562ea3c1e3e6a182caf2942d8c4e6b741151c7b47c9efe',
'is not prime because can be divided by', 2)
('0xd76939d5a65f13341b2999e27ff5d5685bc4f4f649ae23d4159b79f0f607ee10',
'is not prime because can be divided by', 2)
('0x96015d4aa81b5d8fdb9653dc6b7d9bc616cb2585eb735ec08cf1d5daf8885b60',
'is not prime because can be divided by', 2)
```

```
('0xfdd238aabd3e2971ea2061c563598312b494d672a55ea40a3c0dce0ea5e5ab17',
'is not prime because can be divided by', 7)
('0xb9e0725784eb6acd1105873c2187537151fa76fdf208bb2f064ab5f322ec3f50',
'is not prime because can be divided by', 2)
('0x943db2728ac01d24f1d536f1cf80a0114980779530c6e485e61fe81fb9d64c24',
'is not prime because can be divided by', 2)
('0xabb02a28fb2499b021d1a866726aa6eeca87055ff85fc9d890fbb5836124a538',
'is not prime because can be divided by', 2)
('0x9b7bd827b1b830954cbc1e406ad3b46162820d72fa777579130981234debcf09',
'is not prime because can be divided by', 5)
('0xef1152b4929a6716aab5ed05a67832551c408dacad34bd5e8fced370607048d6',
'is not prime because can be divided by', 2)
('0xc14dcbae6ccb4908789d5f658c9e484970c96f2f261ca8c8acbb1b326aaf60b8',
'is not prime because can be divided by', 2)
('0xa0233d06d6e77ab2bf6d71895f56efcead79026f0e5f10d15b50d14e71821c3f',
'is not prime because is not pseudo prime')
('0xabed0a638175d2cce348827a7c4d7efddebe4832ce48688a75265c253a149884',
'is not prime because can be divided by', 2)
('0x9132089b70a80ffac5ae1b0d20d697d7befd91e75d4db34c01dfc9ffd82a5de8',
'is not prime because can be divided by', 2)
('0xee31a66b66a4396ea2238909eca7216c41db34a86a192c9f091167a22fb6913f',
'is not prime because is not pseudo prime')
('0xeb9769d6b90fdd99b681b871674c891bdeda89fe65fc3f9391951379fc494ead',
'is not prime because is not pseudo prime')
('0xd117eaa94ed4810ee60836654bf8740568836c0f79f2e7469f1ae05891ab9c4c',
'is not prime because can be divided by', 2)
('0xbb8af960445d106b8936e733bfcd6ca597f276383b601df44b68a8460fc34175',
'is not prime because can be divided by', 3)
('0x82d95b5ef260fe9b65c236f14709a4c9330b566d58badfa749186b20425f9781',
'is not prime because can be divided by', 3)
('0xb3098bf0985cb6f6e2db9115b57b79960b14ac225cf2e273d3d40dd32f28b347',
'is not prime because is not pseudo prime')
('0x851e658619ea3d6fb878e947be5ed5c97a712c7cc269e6397975d9a1114d4cc8',
'is not prime because can be divided by', 2)
('0x8719486494140b5582ca2c1718fa891c5eeae08dba20586c41951defbfcc119d',
'is not prime because can be divided by', 7)
('0xffacf1c8a863611e5fce34cdee3c6e73e7bd1c2cbee7c3cc3f9ce3b43e22a09b', 'is
not prime because can be divided by', 3)
('0x8a40b232f9a0588d09bf7166264a2774764c2ac5dbd4edffbea4697c7ed74780',
'is not prime because can be divided by', 2)
('0xcc2c0eb09ce19b0407cced10debc722293009db99478e53738eca22fd973e491',
'is not prime because can be divided by', 7)
('0xe3cb5de6016b78d78cd966b8ce36a2aa86ceb6974328cad7934cb8efc9198ab0',
'is not prime because can be divided by', 2)
```

```
('0xc5d8d1a41887f28343e6793da4d01d9fea50f7071e34576b1444de9795b51abc',
'is not prime because can be divided by', 2)
('0x8d0b3eea3c4c55e12c4f4215d97e16a81ba7e1535bf6625d44117b297a106798',
'is not prime because can be divided by', 2)
('0xe7ce035f45d488412ca9f2cb5d98b38c8bc9bcca8941e9d58580c5e93dcee163',
'is not prime because can be divided by', 3)
('0xfc63229e99cd1fef38407dd4c8cb033a8f0f99eb90bb6021db4a316ee51f2154',
'is not prime because can be divided by', 2)
('0xc34b6b65d45b8262e6546be5f15fb65467c479864cf0bc7c0bb7dbf9bb913a16',
'is not prime because can be divided by', 2)
('0xe7447e1efd9f856b8946ef4c252fc48d729ae7b51f341a58642fb00b402e117a',
'is not prime because can be divided by', 2)
('0xe737a29dcb117f3cb9ffac8d2ef1dd65c400a247a71c2d7d9ba46471ebdb093e',
'is not prime because can be divided by', 2)
('0xd54a0c2708e267a96efd4bb4f3e44abf407e4952ffc36e69563f5b3c17686703',
'is not prime because can be divided by', 3)
('0xf68fad26902c933303199558121db39fcdef7a262b8f82a341772349ad30fe95',
'is not prime because can be divided by', 5)
('0xf72d6c6c5badd61f30a5ace103dfc0c3d188f33988875f53493395c58f203328',
'is not prime because can be divided by', 2)
('0xcfb0e3503a4612db4d958c60f741712fb5d483e12dab5f2efcfa59531cfc8fe3', 'is
not prime because can be divided by', 3)
('0xc9238a3ae33fb001372ca9b279005119296bd486f87754e729b3d64b1217bd76',
'is not prime because can be divided by', 2)
('0xaa1d46a3be887ae20592dd61d04da697d28ec3d9e166f47c0fbd44edabc1f909',
'is not prime because can be divided by', 3)
('0x9409c2030be4160f62bbf02a612e3e7921001002a24ba45df37e7c10dfcc3e6f',
'is not prime because can be divided by', 3)
('0x8e714e9b9f8f7b6fd7b49517bb4e7e7cdb635cdcbda4dd5ba5d14c1c5c4f2d9e',
'is not prime because can be divided by', 2)
('0xeba127a05a2da3811c5c5a5c0a3d089c64713eae77f56cbedea9aa22e357ba78',
'is not prime because can be divided by', 2)
('0xaa8e98586ec0491fb82844968caceac791cf01d7884b2964c7e4a3f3e5d77809',
'is not prime because can be divided by', 7)
('0xe6d164c75eb0e7354e92334427de4faf81d831ec21fb83f7b3d4bc474ef0770f',
'is not prime because is not pseudo prime')
('0xffde1498e921f9f54491c66398bf74a19c2ad0983e1c6bf7d89875ccbd1018d0',
'is not prime because can be divided by', 2)
('0xf3a40dc6378f497e08ae47925e9fba1ffb17278b6d417a82a830f2f4d4e0cca1', 'is
not prime because can be divided by', 5)
('0xd8f71796c8bb0740d65ee22c70fa9fdac5f78ebe2d2434f0e98d8e2bca2e05e0', 'is
not prime because can be divided by', 2)
('0xcc11fea08f336a2b63c1882f7f84b8b9227d2dc96a2e34ea4578c9fc6270ee27', 'is
not prime because can be divided by', 3)
```

```
('0xe50f89ad56fae2eb522545e90e079d88a8b913936e9f1893ce72b7168215a973',
'is not prime because can be divided by', 3)
('0xcc702707b4304b4020e314605a43554d56cc1cb6fff32f8c2387fd1412a35473',
'is not prime because is not pseudo prime')
('0xabaeeace64e7ebf5079b9b61feddfdbf34a583f70ab641bcdb14e5c868d0cb2c', 'is
not prime because can be divided by', 2)
('0xcbaaabbd2b6e0f5b6d86af53c88b62db825609d4bbe52b5d22411a6af1fbdf4f',
'is not prime because is not pseudo prime')
('0xbc1bb6954a16277782a16cc21cc464d4a23b0bfdefcf15de106568c186a89659',
'is not prime because is not pseudo prime')
('0xe637c994c9444f16294b9eed6b3560ec5e409fb2e5293b697957a1041f21a5e8',
'is not prime because can be divided by', 2)
('0xca24a48a6efae83720a01f65e945456601c3d5d841984c9a7845fc3566c113df',
'is not prime because is not pseudo prime')
('0xad4c743b548283e4abd35c0515ca234a661443935fe7cb8444da8ac66e3df10c',
'is not prime because can be divided by', 2)
('0x972e44ab64628fc29c8f6abffbd0f1ab66bca4ad41d9e73d5070c9cbdbb46ce5',
'is not prime because can be divided by', 3)
('0xe34fc6500bdc2e0e568625f54016de371d27bb688c0179403835964d8dfe685c',
'is not prime because can be divided by', 2)
('0xb9f4bc61dd94981c4831ad005280b1f85a653f0f77d76b72c91856a3d6016c1e',
'is not prime because can be divided by', 2)
('0x81fe1f6ea2a36a41fbce7b6e529dbb7c35851840b93573cfc699028fe05e0960',
'is not prime because can be divided by', 2)
('0xa44a8079bd3cad45c042478a217048e2f4c82f4e0a064df03e72b7802e4d19b2',
'is not prime because can be divided by', 2)
('0xe529266aa4f6fcca12206e0c144a0bbee7bb8b67c9ecf7ff35c43f6996b910bd', 'is
not prime because is not pseudo prime')
('0x94d3bf94270e6ce0be75fd50d90d6493fb7e8d7712ccc85dff439cda322b889d',
'is not prime because can be divided by', 3)
('0xc85ae7b61014a19d0f790181407e95f540474a086cab191f5c3e0081106d6efc',
'is not prime because can be divided by', 2)
('0xa07af77b8b7c2f21f8696e08b44ef4c76127dd71aeae1b6536e29bb3c90c439e',
'is not prime because can be divided by', 2)
('0x94e491de4ea0c6b0f7d30d1817dfa240a93a276da0005a364ea88290536761a9',
'is not prime because is not pseudo prime')
('0xf687986844a362002e6ee4a4ae9a69d950bcaad3528e0d24c9d33ae8f7b94f71',
'is not prime because is not pseudo prime')
('0xa00e32d98d89ea4be0da76fd1b0d62d0329dbbd6291b25770eec9a82ca3dec8c',
'is not prime because can be divided by', 2)
('0x99943573ee65bd3eb0a95d9297b952692ec15bd76f6b00c79db91d3decdefc46',
'is not prime because can be divided by', 2)
('0xa4de86befa4e949e7bf89170427b6b1f7effc5b4e17caa27f076fb90ed38e715', 'is
not prime because is not pseudo prime')
```

```
('0xbde0656dd90c284b7bc48365fff2df6c79ef6d0784f374ba2cd246764490e8e6',
'is not prime because can be divided by', 2)
('0xf11b3c0d7c1f7119524706a77566b0cce079f5ba3d15a2d16b7c3e77b4e13eee',
'is not prime because can be divided by', 2)
('0x9956b3de89be4c6a6b6a14a51f650612341c4b2c4bdcc5b3598c8fa04ca19261',
'is not prime because can be divided by', 3)
('0xa7f210100bd55f0507f0714c5d7ce17d8114791c5edcc66deba2b716669658e6',
'is not prime because can be divided by', 2)
('0x8e4eec848c62fdcdefd8913d6f1906e10c44d3056394f2b548d2289385d3c6e0',
'is not prime because can be divided by', 2)
('0xb98d276ad24160d03ceb351e6607743ca469fd75d1b803ce4edb759a0bac25ac',
'is not prime because can be divided by', 2)
('0x8d7633b5593ffd0eca00ded959e00eaa18e4695038ff88d16e8ed5caba4bd32a',
'is not prime because can be divided by', 2)
('0xfbb825089c248748cb5761e8818a4462abd91690850aeadfdf3352dcfc9b12b5',
'is not prime because is not pseudo prime')
('0xd41d560a465c62a270f922d816c88d151f118611c7d2c8e2e67791024f12ee40',
'is not prime because can be divided by', 2)
('0xfc68d5d482836d118bfa555e6425ce67289bd20358f78cf05202d0209428ff9f',
'is not prime because can be divided by', 11)
('0xe62a2a68ff8583f5ed223b1bb2cc02781737c7c3f305bd4a8c16ba172924129f',
'is not prime because can be divided by', 3)
('0xb522773c0580721f7ea8d355d702db785bacb9c6f785a01d006739191402b0ad',
'is not prime because can be divided by', 7)
('0xcfd7aed0a0f263cc2984cd3a0aa7132936fdbfe513000172726435b88d9b8b58',
'is not prime because can be divided by', 2)
('0x8676ab3192c5629529789e1864c3dc3f22de8fe50be98ba3b3698cc0072ff897',
'is not prime because is not pseudo prime')
('0xab2ed1b91fa20a5c63e104cfd272132c7c0c155e6e5efff0a4470362d457d137',
'is not prime because can be divided by', 11)
('0x91bcc4d651dda7acdfffaf743319189be45ad4045ab7106add231a7bb8ce6d48',
'is not prime because can be divided by', 2)
('0xf3fc0c2c8f0d1b157d4dac9f66eae9d5b130be7da233a95f3f43ee5435f0ec72', 'is
not prime because can be divided by', 2)
('0xceecff047de2ea493a53666f79a871bc0fb345e04c6e9725776cc3ed321a4138',
'is not prime because can be divided by', 2)
('0xbc36a14d9e037bd330d325124edc0df2f013e538da13c62a1da02c4c9a384e98',
'is not prime because can be divided by', 2)
('0x8e6a1325ab9258d47a188e5b0d8b05079b542a13de67b435e424c13517b6fdc3',
'is not prime because can be divided by', 5)
('0xfc2cb0dff8555c700ec18e6b5044775faf844ac35634a0d0a5d9322adc5e0098',
'is not prime because can be divided by', 2)
('0x95fe8e92aeb724eb12e3bde9c9657d3d90bee34dde2e844c25af3ae0f7d3438b',
'is not prime because can be divided by', 3)
```

```
('0xb075d027c3aab6eb4023f770c8347d52a583dd4b47a783f1880e8e1067072cdd',
'is not prime because can be divided by', 7)
('0xecd4e736873998fc4b6451ae73e75bedbfefe3d2c3b85fd39403ae9ad70d866f',
'is not prime because can be divided by', 7)
('0xcf8931f83c739a9e47687b06a9883e974bc0d1d9ff414a89733a896281514b78',
'is not prime because can be divided by', 2)
('0xc7b1170ddea53eb652c510648f59d957d29b9ce888c9c91e19eb6ac5191870e5',
'is not prime because can be divided by', 3)
('0x9e0a8d5de2b3434925e5d30b8bfc2284f53007f17579dcf0946d804e61e00575',
'is not prime because can be divided by', 3)
('0x98d0625eb37a04bccbfc89bfad1713ed78d01df54784d1731ad983e7c9c54320',
'is not prime because can be divided by', 2)
('0xf8600a1c0527d5bc748da7f3d01fed8723250148ea627a9a02c67a4dff64c1f6', 'is
not prime because can be divided by', 2)
('0xcd54327eaf26af8a80ae5ab90e26cadf51b2225634074780201f38346a6baf44',
'is not prime because can be divided by', 2)
('0x967a1316d5b7dffb46b4b665fc1be13ba04996e971337ca741c9997af3b542ec',
'is not prime because can be divided by', 2)
('0x9dc67daa5addbc308fd1dd8310fc7051d6fbe519e75d671b8ba20a635678a8d6',
'is not prime because can be divided by', 2)
('0xcb0c028b617af1dd69dc476a453b19c3d9ceeceb0b7f2e32f24f92540ef345ab',
'is not prime because is not pseudo prime')
('0xbed82f3d1343a62c8babe6132e3ef2f767e8234bce86c33ffc366f9b119bb62c', 'is
not prime because can be divided by', 2)
('0xc88118243e0e52afea087acf024b7ab0487caa2bbc55611a282ec6fa2db31a1f', 'is
not prime because can be divided by', 3)
('0x9ae10e707bd759111877ed95bf54d0b22f24f84eab6fdc5fd6e98b1f9341b626',
'is not prime because can be divided by', 2)
('0x9a00a772341d3fc0639f855e3ab284e88b8c1a6f235030454127c6c40c2b76fd',
'is not prime because is not pseudo prime')
('0xdf28628d9eadbfe7fe04ae24b493924967906c625922e55e7f76e439a00f3de2',
'is not prime because can be divided by', 2)
('0x9bc6f406397f3538ddfbb3245dfb54db3a4a3ee2ec88c7a9b34b8ab5001e503e',
'is not prime because can be divided by', 2)
('0x991cd308e2dbd73cf1c3ed00d62b81c836a42e3e4e0136b4ec9fddb755387fe8',
'is not prime because can be divided by', 2)
('0xb95bb87c5c4da96fc0db465649984261b6ef08270b6608393827d3da458ae6b7',
'is not prime because is not pseudo prime')
('0x8bb1bb740891ddf7afa1a3e9634506c16974143adf7e3a49afd97c41f5234b91',
'is not prime because gcd = ', 13)
('0xf6f9adb7a12601bc705fd9f575e825ea64750a924937ec9a63d4ca602511ed70',
'is not prime because can be divided by', 2)
('0xaa9dfb4cf9efac525edf54c2379b9ecc5097e1c450ad4340040648620fa369fb', 'is
not prime because is not pseudo prime')
```

```
('0x862cd71fd95b3a27bb989e77ba7ac3dccc6a039a0cdb31cf309e143257eb8605',
'is not prime because is not pseudo prime')
('0xe58f94f5a8e2486152a7d4fbe5cccd96938efa432b39b792655883c8cf35fe68', 'is
not prime because can be divided by', 2)
('0xe49e1ce212bee32f25cc2ae102a9a2f3285a0060271fe4ff4b32c9aa94b85429', 'is
not prime because is not pseudo prime')
('0x8e56dfa1a7c3cb99b2f73224e05fd2b44fc847390f67cc8f1dfe8675fb1ee193', 'is
not prime because is not pseudo prime')
('0xed2ea94e777a736aa7cda328a6403dc9ffd57d39698da375f376b50a5e2823aa',
'is not prime because can be divided by', 2)
('0xbb702acc51d0d09e31f3a91fe8ac29d25024ef690934b56ad9f0cb95c443a171',
'is not prime because can be divided by', 7)
('0xc0e177bde7078db513d24b216ada16af500f31b9bdee359ab50a459541e80fd4',
'is not prime because can be divided by', 2)
('0xfb1e930ccab7c6caa4abdddc183ab1eb8ccf5b54ad9bda37ec5c81715eb86527',
'is not prime because is not pseudo prime')
('0xe0e4fb7f1e31720c957be8845fa396bfca3b095d8e4aa5d66e8bee2dbcb925fe', 'is
not prime because can be divided by', 2)
('0x96aef434cf016c067e06084f1adbfe4981ffd68a10628f897c2b527aa8e65861', 'is
not prime because is not pseudo prime')
('0xf385664fabfd54fadb8d64612cf806ac164c62ae42f18c959bf1c754fd9156ed', 'is
not prime because is not pseudo prime')
('0xa9212e9364bbe448fede9ebfc0d4d2bda219c15b802b4016b7697c09d7fbd961',
'is not prime because can be divided by', 3)
('0x9c41d044f019a982730fa02d9fc65aae40d4e3ae0fdf8e6de3925e1332759113',
'is not prime because can be divided by', 5)
('0xe3a6d433d46124a2632989548af2c3f861c3d47a55392bba8c60ccbbcff3c96b',
'is not prime because is not pseudo prime')
('0xc94e22b13468c12c87fea1e8aaaf710df99b5b01b962c535b729a779eae4b0b7',
'is not prime because is not pseudo prime')
('0x93296129246fc663ebd215bf6277a001ea3144f449ecbb63e8a90e401b122d52',
'is not prime because can be divided by', 2)
('0x965061c7baa4404431d5111354fc3df1c8aab5717ce4d5673b8e7427a854d403',
'is not prime because is not pseudo prime')
('0x9dd47c78a59ad4e7c7eef151b4d066ebc5127f305ec9b56068fa271d6cd1f30b',
'is not prime because is not pseudo prime')
('0xbd4ab842a12ee83e1cdbc1cb941cbcb4096f6c4c761648f2ea08003d914038c7',
'is not prime because can be divided by', 3)
('0xc94b3c6ad57657e37c8864beb13e3410ee319f7eef96aa22923e614212698796',
'is not prime because can be divided by', 2)
('0xf096e1b5dde9759577ce1b5e975fe4bf6dae9aae07f1f5273e1f0a4ef23790c7', 'is
not prime because is not pseudo prime')
('0xce5f080b7c0ba2e5d977cd7014dd9f2391ce95d58a3a252b8b06970ee33c80ce',
'is not prime because can be divided by', 2)
```

```
('0x91ae5b1e38d7acc48ac552e615b81afa25af951700fdf6bcfdaf39938591b855', 'is
not prime because is not pseudo prime')
('0x9af6fdec574d80beeb61bc39806b4092a2d589e26adc06318db2d20b3e0a08e3',
'is not prime because can be divided by', 3)
('0xc26fe090bfbe11dbd7b9b124416347baac23619b11e218a028852d055ea960b0',
'is not prime because can be divided by', 2)
('0xb1212ce2e7a0ef8818376a103d2c0ac7b7012ac2cb83beeef88cca13610868b5',
'is not prime because can be divided by', 3)
('0xb9ca1bc6fe86572308f02f6632de53bb8d957408ef0ef07b360660b086335aed',
'is not prime because can be divided by', 5)
('0x89504521d93ae2db2999d0317aaf97fc0e3fb45a7c034efa39b9843a692fa326',
'is not prime because can be divided by', 2)
('0xedd09fecd0ea7315f829292206e83590f6a557cd11a3578821527cb3e0b154ad',
'is not prime because is not pseudo prime')
('0xcebaca5dd06df93f906f6490a51350e8ec0079d621929bf94b3a941abb875ce7',
'is not prime because is not pseudo prime')
('0xfb095e20185a1cd9961741485921930210 21bf910220cffa1c5ec1b3bea29046',
'is not prime because can be divided by', 2)
('0xc95636ba132a1e0c8a5db97db9df77b64cf09957a3ce3e8bec2809c122585a40',
'is not prime because can be divided by', 2)
('0xadf21238f403204073cf1499b6c5ed81a023093d6c3c4e9fb71e606179ebc33a',
'is not prime because can be divided by', 2)
('0xc35206b9458ce345d7a067c77edd8945db98dfee121ffc1a5ec6023dc0ad8f2a',
'is not prime because can be divided by', 2)
('0xc6f67c1517d6171819cf04babda96e0c3c5c016d721bd824d7f006eb4ea9ff83',
'is not prime because can be divided by', 3)
('0xd93a85d06fc6ef04c3ea901b550e1899e1442befe7befb1008c6b5f708788b49',
'is not prime because can be divided by', 3)
('0xfdcc9018f59e07c09b59ae6189043dabfe0b840211b0f29597be7d411c4459a8',
'is not prime because can be divided by', 2)
('0xb213d5ab3e532f3f37a7aa67e547269fe533809458f7be27cbe27feff0773d43', 'is
not prime because can be divided by', 3)
('0x9c3010901c453293444df36bc162d97b7493ed2ed6040f5678f13e8711c4fe36',
'is not prime because can be divided by', 2)
('0xad7fe59cc0bf0c9557f0515c076e5d18f5e0f9d00b52f4282bac5a039fae7207', 'is
not prime because can be divided by', 7)
('0xca2cfe3f75f144ffe7544b86936225c6fc3ebfabb76b3a1587c4acc5c9dcac93', 'is
not prime because is not pseudo prime')
('0x9dd3ebeee6b45a18aa1c6df054544f7fea7bf595e6defc24777657928ef3d830', 'is
not prime because can be divided by', 2)
('0xe2c9674db2d5ff0b22e44675083b777ddb4edd8d74cb87ba9af2cb3db21bc7f0',
'is not prime because can be divided by', 2)
('0xd4da40d6764bdc7fbda771e737a8502b01cffe931046ed7f71a4e1562aa9265d',
'is not prime because is not pseudo prime')
```

```
('0x8b6910bc586c79be2d2681aea596f924bcc7c174a67e443ce983922e2c982a2c',
'is not prime because can be divided by', 2)
('0xef2f21d9b9dcfde0863f4a781564b23f196e2deab97e26b769e34b424ed7b3ed',
'is not prime because can be divided by', 3)
('0xe3be69ce082c917fa9b146f6527f2180f40632f14341bed0c3337dfe73b20349',
'is not prime because can be divided by', 3)
('0x9cde677339c6762c553ca93b669a49979ccb304341c5dcc9520a36d622c1ceb7',
'is not prime because can be divided by', 3)
('0x8e813354f5584c3477f2247310ac71b0390ad5acba3ca0db6c36bc9567967609',
'is not prime because is not pseudo prime')
('0xb3ed5bfb783aa890c4b43b06b0f98b695b3667b14abb7be2bf593cb864e6ceb8',
'is not prime because can be divided by', 2)
('0xdb5bb6a1f0f6cf9d3bb684d53c7ec4e58c27f8d8902a53358a12876d226f9e91',
'is not prime because is not pseudo prime')
('0xcb7fe6b79c5ec2fd70b2af261c95bf328e2aabb4a2d3fca646aac06f18bb9434', 'is
not prime because can be divided by', 2)
('0xe2d1686ce74830f932abf0acf0f3f9dd29c3e4bbd94a697243d16503fd1d0a9f', 'is
not prime because can be divided by', 5)
('0xd63a5c08d4586101d480ec6ce31d2a469dbbe50d3faafc9eba1f1f5dba455d72',
'is not prime because can be divided by', 2)
('0xc30708e9b895a99788404578008bd11f1fcc6375148df81b4a874af00bbb973d',
'is not prime because can be divided by', 3)
('0xacce43d6f197907f7736ecd2758b6db6174a43efa768e8255b1f128024de09db',
'is not prime because can be divided by', 3)
('0x91b1e5b69f4ccf81aef85734a9e6fc10ef6e3eafabbb38ee65a07f0ee3d466ca', 'is
not prime because can be divided by', 2)
('0xd5b85c50097160302ca1d61810afda57a182814a50e7ed2a6269d9c3234d153c',
'is not prime because can be divided by', 2)
('0xffd738185d9e58631f79d3d597ff39b46a8c8b422aa66988a9a2ab1ace4d1ae0',
'is not prime because can be divided by', 2)
('0x9d7be206dfeff4c06dcaa3923e328147cd9f6245f097d4e34ced8651529fa94a', 'is
not prime because can be divided by', 2)
('0xcd4712aa8ed5435bea8892bd75753ca290422e25f5c4e8927d9f670e8ea42f55',
'is not prime because can be divided by', 3)
('0x93227469eac22d80830703da6045c8eb864d31ce2f0acddbd4ce7c55f4dc578b',
'is not prime because is not pseudo prime')
('0x963724ea383b30af9c2fffa6ee42ebb51c4d44cfa6a93bac99c0e8bfec3395ac', 'is
not prime because can be divided by', 2)
('0x9b554ed919276dcf5e6c1c5db4f73040cc684f5fddd3b7f8215184fa82b0d1b5',
'is not prime because can be divided by', 3)
('0x82c30b541a53e419189e25dbfeaa90a7740ba05352fbaf9cf3e8fd64e7a51887',
'is not prime because is not pseudo prime')
('0x82eabf0e834056f4bc76f1f0882433ef2364c3f87b1fa1be24b2af92973090a6', 'is
not prime because can be divided by', 2)
```

```
('0x95cc6aee4711abbcc0e3f1e35a642ef4abee438894afc411a7acbf89f3fcec16', 'is
not prime because can be divided by', 2)
('0xf4b6d6f370b547a08c4e38f83ef0c720d7e640eec11c00fcd33828fdf32414f2', 'is
not prime because can be divided by', 2)
('0xb0cb7a4c61d5b4f4a267b03c36a677865d4bf707d74a54785fff0d4e13670105',
'is not prime because is not pseudo prime')
('0x9a3182c7b29d939c39817dec84fdb80137af7f6a47d5e9353f5275af58754567',
'is not prime because can be divided by', 3)
cookie_name: JSESSIONID
cookie_value: kkA741SGglCvDaBu3G5jdg
n1:
0x94421519f696912740a11f3ef4c28850b6dfa5dc83925e972babe26ac78327d9b1d
a2e0f950fa08ff713656d13548e25f5ccdf0d2029ac570f25cd59e9fc1aab
e1: 0x10001
p: 0x83c38205a91bab4f3a953f56c0cd71d671617dea1a8d5ea5b699cde43fa17881
q: 0xacf9e9b0c2d0138fa60aa71a1c3db70e44fb21878d605cf3dfcd8e94fe935b37
n:
0x5907fccd3125df44ae6fd17b7b33ef6257e8332ee5c6bf5b973d1820916344ccbc5
4c6ff0a3821f66f04bec117023df4d0420de5f8a0b015d0ec56844199beb7
e: 0x10001
d:
0x52dd1950cdaea7186096984daa84d308203370f7f44ac02dfa1c95c93228478e7f1
4d7944629688d332def1af46860c544a502e1e57e3a0929da3c7365ac5701

my random number:
0x578c6ea18e1ba25eb16bafba55b772e8539376b1ec3b9ff64b305016db50a958895
950ee5d5d086b2b11f3135eacfec80db8eaa2c22efe3f9d1a74bbb63e8f11
key :
3167b700ebdef3c8f4be3afc5e6bf0c0692228596a852b870a26cb23086d81aa8087d
882fc528bad24a0eeb5fa911c4c68667abe0a8536a64c8a0ddabe91b6a
signature :
7a6d817dc4862b34aa8c8ba44bbee935a3fec2bc3c61f98ab8648c5e2ad71812c2154
1930f6552549db8795cf2b0f2d3b947ef3fa479b04152c6cd18ca2aa3f0
modulus :
5907fccd3125df44ae6fd17b7b33ef6257e8332ee5c6bf5b973d1820916344ccbc54c
6ff0a3821f66f04bec117023df4d0420de5f8a0b015d0ec56844199beb7
publicExponent: 10001
Response from ReceiveKey request:
{"key":"578C6EA18E1BA25EB16BAFBA55B772E8539376B1EC3B9FF64B305
016DB50A958895950EE5D5D086B2B11F3135EACFEC80DB8EAA2C22EFE3
F9D1A74BBB63E8F11","verified":true}
```

Висновки:
Отже в ході виконання лабораторної роботи ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA та практично ознайомились з системою захисту інформації на основі криптосхеми RSA, організацією з використанням цієї системи засекреченого зв'язку й електронного підпису, вивченням протоколу розсилання ключів.