



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

ЛАБОРАТОРНА РОБОТА №4

з дисципліни

«Криптографія»

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

Виконали:
студентки 3 курсу ФТІ
групи ФБ-84
Гузієнко Вікторія та Ляшко Маргарита
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Завдання:

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 криптосистеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Порядок виконання роботи:

0. 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.

1. 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 $pq = p_1q_1$; p і q – прості числа для побудови ключів абонента A , p_1 і q_1 – абонента B .

2. 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_1, n_1) та секретні d і d_1 .

3. 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 і B , перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.

4. 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 $0 \leq k \leq n$.

0. Хід та опис

1. Перед початком виконання лабораторної роботи ми уважно ознайомились з методичними вказівками, щодо виконання лабораторної роботи.
2. Написати функцію пошуку випадкового простого числа заданої довжини, використовуючи датчик випадкових чисел та тест перевірки на простоту.(тест Міллера-Рабіна)

Для цього написали такі функції:

GCD() - найбільше спільне кратне

GenerateP() - генерує число заданої довжини в бітах

FindDS() - знаходить розклад числа p — $p-1=d*(2**s)$ — повертає d s

TESTMillerRabin() - перевіряє задане число на простоту

3. Написали функцію для генерації простих чисел p , $p1$, q , $q1$.

GenPQ()

4. Написали функцію генерації ключових пар для RSA. Після генерування функція повертає секретний ключ та відкритий ключ

GenerateKeyPair()

також знадобилась функція для знаходження оберненого елементу

ReverseE()

5. Написали програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B.

Encrypt() - шифрування

Decrypt() - розшифрування

Sign() - підпис

Verify() - перевірка підпису

6. За допомогою раніше написаних на попередніх етапах програм організували роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA.

SendKey()

ResiveKey()

7. Перевірили роботу програм для випадково обраного ключа.

1. Значення вибраних чисел p, q, p1, 1q1 із зазначенням кандидатів, що не пройшли тест перевірки простоти.

0xdeb77d6b9e5438997b66e1facab2123576bd70e0eb292d685bfa72047f2cb5b7L - Miller-Rabin test failed.
0xa22ba1d5c1fef98a72647984f124b6f0806b6ed9024227e7d328103b9ecbdb67L - Miller-Rabin test failed.
0xdfaa4f99390334b225285a722be6de647b0c4beb6069442a19ef1e501f1a87dfL - Miller-Rabin test failed.
0xe3896ca5d22d18a2aa26aa36678fc9d9b89a5b3b08c5974a3064ee11368e3ac7L - Miller-Rabin test failed.
0x911ee8f5f8bda733b167ce48346b68ca3d5d06fd4244293b8c1cc07736ecc959L - Miller-Rabin test failed.
0xad102f218e7aec5bba640f47682350e87f0f1b0a8e7856755d91a23aff042e51L - Miller-Rabin test failed.
0xe3c94f2d2b5b38df345b8796a8d2ac608f317443c2341b6b7c3f9fee24fc3be1L - Miller-Rabin test failed.
0x98f243c5a7d9fb191ac5ef902662fcd9e5a57728b25b9b17ac7a818c46193c3L - Miller-Rabin test failed.
0xa47e447d06a640a596947abeaf5abec16de611923c9ce2c20104c9ca1e0db9bL - Miller-Rabin test failed.
0x9342f15c36222e299045eadafad52b54609c6d1c0f5c6cb40bd7806600c8acbdL - Miller-Rabin test failed.
0xe8bb554b587aac7e3433716fd11616d18a95dda61ae99d849b27f6aa60fee45fL - Miller-Rabin test failed.
0xf29d10d23b79934361226c36cf16fc5797220fcc3477ade513295bbddf68f06fL - Miller-Rabin test failed.
0xc99c389c2196518d3f817be132af2864717b3eae3a5f3364da7bce412bed2b5fL - Miller-Rabin test failed.
0xc7f128404cea6d0a14c7141bc732d8d5cea006af9011e9774842db741431b02dL - Miller-Rabin test failed.
0x9b64a09a8e5318d819a163b8c840c3b3857923a10b87941a58855963986ce971L - Miller-Rabin test failed.
0xb60837eef5e15547b37aad5b9cac042b592bf66785db9774b5256754dd40d471L - Miller-Rabin test failed.
0x826c520f6b998eedbe67fde346f485b1f3487740d86c61106f712879051a8c7bL - Miller-Rabin test failed.
0x8b4324701974b518d7244d3afdf58df356640fc469c202b32be93332e4f3159bL - Miller-Rabin test failed.
0xab727b2fb445bd028bc7b9e622c9ee33e080ad54361c09fcf45d6ef6457ffadbL - Miller-Rabin test failed.
0xc973982f52d5111ad9d24e3db04efe2d1f2134b093aaf87b27ca0f5c73023785L - Miller-Rabin test failed.
0xd97a8c897fa2f010774ce3a822626b5199371d5862d0853617ea722b8063a90fL - Miller-Rabin test failed.
0xd5809ccaf2f0d0d338dcb21af2b0d581775edc25e48bce93a721ed0f84c79ea1L - Miller-Rabin test failed.
0xaf187e8bd55dd58991f4081d793a09ac5d66a3d06f6ded9b2439a9f7e2f742fdL - Miller-Rabin test failed.
0xbca9bec5547a1fd43075411e40ad619756aee15d4dfdb0bca767b7797d266b83L - Miller-Rabin test failed.
0xefccc4a66ac16f7778b282c0acbaa7b269104cf5bb2c865827185ed696aad607L - Miller-Rabin test failed.
0xb643cb3b8905033e375e2cdc6b98a57fc1cd8c72753d6f4881c3f2f278e04311L - Miller-Rabin test failed.
0x9ce6788fe9b21723b7734d474184eca620fe780c1fd9d80f9ac804fc6ae3b5f1L - Miller-Rabin test failed.
0x997131f09b27bd719899264f2fe2b3343c4c1578a326c991cc1639383c367e39L - Miller-Rabin test failed.
0x8c70a99e9f3b13a85c80f489b32ee9b68e3c87e2b242e249271f306f6f82f353L - Miller-Rabin test failed.
0x830c274cb39d3f2fc7da483e6a2d39c3a5de357a6e57fa32b0767d958ffb4d59L - Miller-Rabin test failed.
0xe51fffde16eebb36b005d7453db42991b0c787cbd842f53c47db2b7b97121303L - Miller-Rabin test failed.
0xf6608b95ffe03a5ee4eee4329863119b978a8fee5446a08560f1dbb0de20bc93L - Miller-Rabin test failed.
0x88c94cfa71c39bf4de227b095170c033094248109bd96f82f98a903bfc2d2cb1L - Miller-Rabin test failed.
0x9a5a7f813b3a9c24f667c94dc03dae677cf2186dbb60bccb121f1341b368a64fL - Miller-Rabin test failed.
0xa75a3c2c544fd25cb2b3394abf5b127ba8f53fd6201053d66b0aff92c5b2a1b9L - Miller-Rabin test failed.
0xe62ffca7bd0b459242f76799a382a58c9ba50964022ab0be5a0fc30a453c7e03L - Miller-Rabin test failed.
0xe35c4b696ba94cfc61a582e0201454f7879f33a78141eb04370ec54eec1d3631L - Miller-Rabin test failed.
0xd5042e7def98c608018a15a6ca99e01498a779c2ee2d3b1957a006cd7f9141a7L - Miller-Rabin test failed.
0xafd492a70ec16c70b90bd2885274e068f91251e9c4244e3c82f59b441fd382cfL - Miller-Rabin test failed.
0xf52b895eaf887904d64fe073581097c4db61d4cdad4fcbdddf37f058eacff311fL - Miller-Rabin test failed.
0x965ec1344fc3db3c7038a4527c33bb18e79154d4cef3747cc082f86d0a40772fL - Miller-Rabin test failed.
0x9004b12fec4557e94beebcf49425124e3c99a2651bd00aa98248de3fb45aed79L - Miller-Rabin test failed.
0xacd15321d2867ac08592f09048d1f1193861ffdaa08b37f2a8283b0ca0d8f00dL - Miller-Rabin test failed.
0x94815a848239840a1a880aca6906ca11b7756edd538b2394a2a1decf0cef9293L - Miller-Rabin test failed.
0xca3e46fd5d6475b7ba1b7503be932d056758f27bb29187dff1e0d8317ee1ea85L - Miller-Rabin test failed.
0xdc3e6e8aeeafdeb1973a6f03aeb801f689aae2885aeb8f4a02a8a98c24414b3L - Miller-Rabin test failed.
0xa763e6a75f2fad9f024346a6272e8ddfdb489533c23e91cfcedf58ea17799e91L - Miller-Rabin test failed.
0xa261b382e222e929757f125096db98e775afe1e83176dbf2892eaa50d6abdbcdL - Miller-Rabin test failed.
0x9655390adafc653a3fb562d5285a263eadefaa93c1152ea014f19c16d5cdc6c1L - Miller-Rabin test failed.
0xefa484eadcdc169868eb31a2b1cb730272f7bd22c6cc85768ed2a06f8ffed54dL - Miller-Rabin test failed.
0xc2c361ff71e80065613712ec85b33db92c84d7f0453e2302f59b47b037c99101L - Miller-Rabin test failed.
0xa60b2ea32059d3de48cbd7e7d0c87345de409b052322b7bd78b1ff2f905c8269L - Miller-Rabin test failed.
0xd310bcd4730251ea703c1ce74b12dcb5ed9120fee081545e6efa2f7bfea32093L - Miller-Rabin test failed.
0xea35a30a01f28339ad281b49e6b24e51dc6633dc66758e70edd30e46986f132dL - Miller-Rabin test failed.
0xa677910f6dc37357046d7b5b8b7ec108320dbed26f118ec5e6d050cdf61c5e7dL - Miller-Rabin test failed.

0xd60e805431aecfd37ce7078c8fa812eb0ac329c9343ba7c66522f14a0fa2cdb5L - Miller-Rabin test failed.
0xfaeb060582fdb5b33e40d5cabd6cf198379f1c611dcc317d3503168477a66d1L - Miller-Rabin test failed.
0xe5c4970cf19df09e22318c2df0952fafba12f1a01f492ef6d325d4c481c29653L - Miller-Rabin test failed.
0xeb117609784ceacdac36c21700b1052aa14f63c7f281f88f361d3dfac03489bdL - Miller-Rabin test failed.
0xec564d5eba5d68329d54994532dc7a9f62d8a11c134dbcd84e864e057b93b015L - Miller-Rabin test failed.
0xd7f604bfc26bf50f1d29a080b08a5d834e29b76015b5e046fbdad6007016b389L - Miller-Rabin test failed.
0xb854e35d0b74ce9d60789421dea5c209f328143f1f612abde9fd4aaac92fb2b7L - Miller-Rabin test failed.
0xea38e6f3b257c33ba4605d6d63cad24cef07f9d0e64c505d576b71711e23f85L - Miller-Rabin test failed.
0xa325eca0d34f6f1b54b36265bf704e66b5e81f92d810913e4f8f78aa13f6c4cdL - Miller-Rabin test failed.
0xd6ea1864a106decca3c5bebe68d43f9fd2867ef1c53ec02973e174ca26ce5f7fL - Miller-Rabin test failed.
0xbbb0be2ce15fbf317f2247e4cc942c809d214e33a3e5af076a39ad2f565699b9L - Miller-Rabin test failed.
0xa35ff3c3d3bebadbc665e83d846a72c43ef119989fd9d71e1c09ff62481a275fL - Miller-Rabin test failed.
0xd5c20ab76f233fb9d8ddd3b0ba2f108bf4c947258da1f2bcc73ffb349128cf1L - Miller-Rabin test failed.
0xf261b74d4ec3fc2dd7e39feb99e2895c492db1e73773255294acf4b1fc79f843L - Miller-Rabin test failed.
0xf2e686aacba18e2bbfc1d9c31f1666be7a9a7c2ae7485f505c6d42bf3267de2fL - Miller-Rabin test failed.
0x9c67784d751902866d52e1d5c1a5042f66e1d701e4738f2b6207c8e963181243L - Miller-Rabin test failed.
0xf1082a314d4836a3200b7494bb27846135f60b737f89794f275eee5d2245ec65L - Miller-Rabin test failed.
0xe280d9f7886e72cbb129c0d0853c2c99bf60072636d777cec5dfdd11632c17bbL - Miller-Rabin test failed.
0xc035c6a2eda8a1cfd45af42eb38184ad947453916191a41b52656abb756a886dL - Miller-Rabin test failed.
0x8536550cde5b80b1a99f59c972e0f0b4075f06fd9c423a063ae2c04945e5d0c3L - Miller-Rabin test failed.
0xf384537ddd1e610e495e44b6fca3540f71ca85094c0872e808bfd191d5ba0d51L - Miller-Rabin test failed.
0xe92e2930ca8ab2d1e1a84ff2d503777ab7c22ef220f220989085a6f3dfc67fb1L - Miller-Rabin test failed.
0xa94a62516f1c00133dd080b18ca2d2904794eaf8cddc571a623889525574cabdL - Miller-Rabin test failed.
0xe8658581398a0e28a0a5d1fa8274920ca5364f69265a019ce755d5bd8639c069L - Miller-Rabin test failed.
0xe8e8d1f2612d1a38b02ce5aa1e0ba810f629b2ebb436552c0d4601b93d6f0857L - Miller-Rabin test failed.
0xb895d3b17e651cfa2e72e3beaaedceaa47ec38f150d711e9f3fdb222e93159dL - Miller-Rabin test failed.
0xa71df95205d6df11ced6a94b6567433460445d7352efd4348157d36d4bb89f33L - Miller-Rabin test failed.
0xb5b1e586b9d32ad1f92a796a7aa132e98cf6710eb9322757332d24deb7e90af9L - Miller-Rabin test failed.
0xbf61a1e7b2ea5048993ccf9eb467051a164c9c29ca2dffe0eb1a2b6649ac4f91L - Miller-Rabin test failed.
0xa27e2cced7e76c30336c1b6ec2b421fc4a28288717d0dddc797448dc97f9e089L - Miller-Rabin test failed.
0xcb71508ca471eff7d612988377909ae6dd940e7272b0e46448e0453d80821955L - Miller-Rabin test failed.
0xfc3c50d1449c2856e5b4d2492d03499299d90a25821c16e8a75fa4d177008459L - Miller-Rabin test failed.
0x81148b9a77bbb83cf211dc7a30b13b37a96c5af9522b334b9b58661374da1853L - Miller-Rabin test failed.
0xafc21c81d60aa89716e23686f0c5008db84ac685ce9573c21e5f7b82216d09fL - Miller-Rabin test failed.
0xff6af6b13439b984f5053d7d5f013707db45425131599a641c7daaa337dd596dL - Miller-Rabin test failed.
0xce228b942386438019ba8f09d0972056c578fd8b7610943e8b332c3882d58f7dL - Miller-Rabin test failed.
0x8b1879f43a84f397c53de3badb0da662e85cd466075d8bfe518557dfbf43962fL - Miller-Rabin test failed.
0xbc26f7d291bf4d1c41caec865e90ff3e6fcb0edf6bdca2f751c7a5a7e171b4b5L - Miller-Rabin test failed.
0xf3394f34c4317c40dbf86f471d13bfa22af0d1045ab5b3993ec7bc342610e9afL - Miller-Rabin test failed.
0x879f7d59134fe62b4567cf9776205cea1329341e273fb94e9a99e84531bec903L - Miller-Rabin test failed.
0xb7eff1815e2efea01fbc193ba33682cad1fa9084d685c54384a4a154101bdaf9L - Miller-Rabin test failed.
0xec5bdaa7a14810addf9d3391861f0a043ecc44d29f9277780a1cedfeb3a6709fL - Miller-Rabin test failed.
0x9ea27eb522603968dff405d748a7eb7b1fdb619ae4534be4fadf7662aeec715fL - Miller-Rabin test failed.
0xb4335037a26cafa4c558b5c897ad003cdfead890d777b9ce93fe5d31b2b50ca9L - Miller-Rabin test failed.
0x96f6833d2848277b1ac9dea7fd9258489375b8239f7dcefd3601258a8b18c0dL - Miller-Rabin test failed.
0xe17a0dcfa4e213d971e4997991b453dff38ee9e9f64d42f70e0a20cfd02d72dbL - Miller-Rabin test failed.
0xa643c57df9bd8d39ea608774eb0b996638920e7d3405392ded5ba6bc8bde267fL - Miller-Rabin test failed.
0x9363e515563e5f2a447507b054f07f5bf00a324644aade5871bddd84f9675cd3L - Miller-Rabin test failed.
0xd2caf9e1e989424bfafaa021c37a74170f058042258b0abcc38ebc2caeb062efL - Miller-Rabin test failed.
0x836045d41ae5175acffa5e894d00ed1a3eab8e537155a056ca76ffc77cfc3cd3L - Miller-Rabin test failed.
0xeeee3a919a013723cea3536e94e59b2686a0679044af15f64fbc90ea9b52fc53L - Miller-Rabin test failed.
0xa357130320e987d8ba38ce30883d0339ad1dff2d97ff713a7a84ea132b34d5c5L - Miller-Rabin test failed.
0xb93f2b7a184334b84432325cc5df931ab18231e47b0f1e5b91c4bd0a3b2193a3L - Miller-Rabin test failed.
0xc3fc8d0439307a3d9abad0301007ff07226a93af0eff718885d91a40aa3b0a9fL - Miller-Rabin test failed.
0xfbb28635b31dfb95de44bf40697c6d1d6aa521a7143f39cd2ca9f1a21d2b210bL - Miller-Rabin test failed.
0x807d1917ec7287e7679f3585ae69ebba4a8f529d2f21135cdd1f5da8321ecb27L - Miller-Rabin test failed.
0xeba8d499dea25c87b257b47d5e1b5798eabad42d0b058a5f2465d3c10fd32013L - Miller-Rabin test failed.
0xe12b18807202fb8e654f31ff8a612c9448e6d8cbac18bac41f8e0e5f95c193cbL - Miller-Rabin test failed.

0xf0d445b216da7f96b9a1a884d6652072c68c6766b5e17891a7455199f6df063L - Miller-Rabin test failed.
0xb057911564b32d67b332ae5a539796878e20b14b6982476615641131e4058935L - Miller-Rabin test failed.
0xdd6093ffce0b367d16577d375fe5a59b3013df40a85e9e646dbb88974112972fL - Miller-Rabin test failed.
0xdd09e2a3e4e25e8051e14684f34c565fd923e277e156eed53503bbdba01e4e57L - Miller-Rabin test failed.
0xcf681d2f475204167d5c025750cde9edba68d8615da016c57c099389367e6049L - Miller-Rabin test failed.
0xfba81f2f1d6cb3cd28dfd45f2941055f45a2d2f1a093310fd77e6672928aab1L - Miller-Rabin test failed.
0xa2f8bafd3611b3b647b0705e342111502b31371f691a957d262901c8a80cc2b9L - Miller-Rabin test failed.
0x87ba2d0d20cff6e4d2d39afda057c321889c9e94fdc9d8f46e9d0b897a3c9L - Miller-Rabin test failed.
0xa82279dd3a5a949518ef808f7fed7d79e51d4a2be800b4ceea886824bdf01623L - Miller-Rabin test failed.
0xc6f19153aab41ebca00c3b79ae3033c9aa164da065c8a05b71b15c8caa0e1f5bL - Miller-Rabin test failed.
0xe45eebdd6b836b28d09a743d06dee7d2126246ccc0200f0dd0d6852e69212f05L - Miller-Rabin test failed.
0xd6c8f8aa2be0b43ea7450a14a0eed79190e01f330b13d05a69631f55f9b2d4efL - Miller-Rabin test failed.
0xcbed3458ba62e6103e686e979edaa4a9c02804ced115f4a289b452fe1eba0649L - Miller-Rabin test failed.
0xa6b315e2f6d3b542215ad85aef92c841104691567d24833ecc2f9d9d11f68b2bL - Miller-Rabin test failed.
0x9420731fab6d09437621ce9710adc0370b515f2423f76b71ed9484ba5bffa3c5L - Miller-Rabin test failed.
0x9b96c1f70ccd4ecfd06efa84c053178ed4a36d05f06ba31612a9a5c85083bfe9L - Miller-Rabin test failed.
0x8d548c1450f80b01de2edd8b7c04e6d60c4ad199f7d4bbfafb6c502452bb51abL - Miller-Rabin test failed.
0xec7c64580e3dc3b513924f4b7ac9926f1a3de57135841473a6ef66789beb5933L - Miller-Rabin test failed.
0xee21220c9dbaa8db66a14b3fcf824e3211c30daac46a52792e7e523b11ea17c5L - Miller-Rabin test failed.
0xc04a1993a3eef6bb7abe8195a25304161136d9957d2d4bb8b9ee47d9b3ecc93dL - Miller-Rabin test failed.
0xbb6dadbea46d175257a706e2da7f59b45232e200bfd67d072ec079993d9e1e77L - Miller-Rabin test failed.
0x85e657b994b0ad8fcd553d9318be010fdc63e3f71a7daf52a85a18d5ed4650d5L - Miller-Rabin test failed.
0xcbf8db9311f9a271be08726ffce3f2624332f66161a8786bf74c8fa20c854a79L - Miller-Rabin test failed.
0x929c9221cc21782149543257d32767f1d75668a270bf3e4003222f54f78ba0efL - Miller-Rabin test failed.
0xa7f9ff4f9c2179a18efe8ca6c909192d5f9676b50bf3a0d0074f1dd03ce9d7d5L - Miller-Rabin test failed.
0xf9e8cfb5eed09911458a555d46f6564d43259f69c210d4832315366b7c3454dL - Miller-Rabin test failed.
0x88c779233875550675c6c92a0cb4d7235dc29679ff649fe67e1f7cb4e75b3237L - Miller-Rabin test failed.
0xbda917afe3c9cf30fe77f89b3564cc7dbf0d3f5c4530688a21102bdf1bb5b263L - Miller-Rabin test failed.
0xf5ab0ccc46e25326d73030c466baf4f3be8684cc8dabc5f163720a0946c56bf3L - Miller-Rabin test failed.
0x8cd00847686f66aef6d635e73dea099e39428728c3b8dbee0e4ea90495246b83fL - Miller-Rabin test failed.
0xf9e5a2bc5a3edde1d113cd1d876d4adc53674c879938ed6347057c1df2ac889L - Miller-Rabin test failed.
0x85e5cc7beb9b7eb6a2b89179fb31c9c81d83a355c2a99e95e7c614d37f216007L - Miller-Rabin test failed.
0xa49a396efa4b72cb7e16920ad16364582a82f60a272510b089ab0bb566c5c95bL - Miller-Rabin test failed.
0xbb247c3b6d8eaf11b5fc2b484e346e194ad1f7263f691a44129299aeadeea307L - Miller-Rabin test failed.
0xb4b8fe964481c260e2b61e6590cc4477a91997734f09eea103a9a4e28570fd5L - Miller-Rabin test failed.
0xd88589ae913f795cca59390870589e1c3d923abcfdbabb23236adeeb0f34e1491L - Miller-Rabin test failed.
0x9a2196e626619590add383683fbc2dd41a50375cc780f6436481aad098d3b069L - Miller-Rabin test failed.
0xbd31390abe2be02eeb9ac8302ad8f38511d9fad0a340805e90a40002a3cffac3L - Miller-Rabin test failed.
0xb829d0470f892d343df14cbefa213732b87c9db82bdca7672ac283ec3819168dL - Miller-Rabin test failed.
0x8e3fede3fa25381b63bc32f42a54256062c71f691ebd5da3f1d3901aa00166ffL - Miller-Rabin test failed.
0xcdaebc33435098f8f195f9036d04bdb381b390f1dbc6a9cc88c537e89415a1a9L - Miller-Rabin test failed.
0x84719b334d5154e472ad95baa9baeb7ab4eebdd031e201e08fa02b182069cebL - Miller-Rabin test failed.
0xacd65f412bbc1842618976607ac3fb6a83d1f86eab895c9a6296ec279da7acd7L - Miller-Rabin test failed.
0xea46c5172073ef7cb6c9e4aba0d4007a83455c5e24dae9b62cd79cdc849bae0fL - Miller-Rabin test failed.
0x8cba28e30ca9bfb56386550d172cc556adc25d2a6334d076062685a74a49ffadL - Miller-Rabin test failed.
0xcd97fb89d1561ecd42265ecfa4472a63fce70bceac1f7aba4c090a99d00b517dL - Miller-Rabin test failed.
0xb4497da31ee088057a49e07bb73538e481c73cfd13492a7ff45a36a19c2e4947L - Miller-Rabin test failed.
0xe82ebb6ff678a059b1cdc90643493c7f27fa10313da54315878b3cad8c655e61L - Miller-Rabin test failed.
0xc3dd64dbe2b0c3d79e400fa2577994d889f30c19049c59e04d5081181c9c6b8fL - Miller-Rabin test failed.
0x99b1c9eec6f5d358466980e992cb2073f18a5679c956900888bb532f48a73061L - Miller-Rabin test failed.
0xb75d039dc887aae58d0bfe61c7402dd4bb39fde5f192af64dd66b3b901bd7a2bL - Miller-Rabin test failed.
0xa6ce788444cebd785952eea204a8cb6372774b1da20ad711984649d6e35fa189L - Miller-Rabin test failed.
0xce99f9c0cf9d4f6d379d5496fe216de0e0b31b6b469d9a3041c9baa5dbf4c1efL - Miller-Rabin test failed.
0xf9e5e9390b4ff223e63e3e1ba4be1d3f66b085aef739c1a2071c3bb31c96dc87L - Miller-Rabin test failed.
0xeca662ea4bb4ef82e5edd7547ea4de83f40b45aa4314279b88666856b728817dL - Miller-Rabin test failed.
0x866d16556ecca62a6cd324279b5a78251af51f71ca302004eb382ee4d66acecbL - Miller-Rabin test failed.
0x85f986bef72ac294749986bad21ac9f0ac2e010546e0451264b93d377f97b4b7L - Miller-Rabin test failed.
0xe3671628fa13d2a77e32790ddc31778826913d9e73d93e9133d5ea92263c5ddbL - Miller-Rabin test failed.

0xfa5dca403b7d6185a5ad54828b113da06a45438b0b7cf110cde92fd6330d3d87L - Miller-Rabin test failed.
0xf4aaf83c40e7663b0a946c2bf3a6d0c3726b27dca290dc40aed2883e4da2aea9L - Miller-Rabin test failed.
0xe8973561146f7d372663537f44eea019dba3ab282ba772408b2d4bd961283a29L - Miller-Rabin test failed.
0xbfe1a824f394735b0c8a092c764fad66ee5371dc3fe4f19a2209928abe4e84dbL - Miller-Rabin test failed.
0xa98df12341583abe5f84f13b715e5f1ff5b60ea7b2dbed96ec576659ee224213L - Miller-Rabin test failed.
0xe16f89a370428e7a83035714ee67dd745fe33ac35fe82430a69c44472d343c0bL - Miller-Rabin test failed.
0xbce2039663c942cf4e036d01d5802cb0842f5b7b813c3beced5b4b2de09b06cbL - Miller-Rabin test failed.
0x99b322cf826edee79904a24397564587b0fbb8a90eae9957fe592ec46c4e47e7L - Miller-Rabin test failed.
0xed5eefc4cd07bffd7bd2401343df58c5e70509f671aaf7ff78a41c56786b2e0dL - Miller-Rabin test failed.
0xcc126f793b237d604cf1bce29e68629c86b98a7e7102b472dcf2f9e979d908afL - Miller-Rabin test failed.
0xbaefd71eec1814a441aa8acdf8e06fd3f5bd888b5b1e2c415490b545c24bcadL - Miller-Rabin test failed.
0xf46249af7e8e9931520cb075bcc8520f8f18e90f54bbc3454f9316a67a5d8f6fL - Miller-Rabin test failed.
0xe5708737619041b51f5f130ece6f3a69173152c69a75e0f10cbee82b720a24adL - Miller-Rabin test failed.
0xf3c325186236ccb0164158d5ff7a75a1c983a8a02f1c6252959b46b86d24947bL - Miller-Rabin test failed.
0xb4cad06279914df92d2e8ac3b5cb9120ce396f384226b028651da4db6d2d6f61L - Miller-Rabin test failed.
0xfe7c28cdc94042b152199507948da2d7d0cf6bb21d0d6374053049e7eec11f07L - Miller-Rabin test failed.
0x9634d9d486c480f13cb04059ca9c0606fb62b50ef09de704af58401bf76e30b5L - Miller-Rabin test failed.
0xe348e18524714230fb5156645391648528326653ca35e07302145773a9ede1b5L - Miller-Rabin test failed.
0xfaf528e1bb1df1f3b676ae9b29bc0c33c8a4ef4f4b91db7196a0535562311301L - Miller-Rabin test failed.
0x8dd2a0580f7d3c61bc41c4284bfb6080e76e415c040c96be6110f2c1212e33c1L - Miller-Rabin test failed.
0xbb814f46a3afbc7ce5a49e99800561fba7c0bdc226e96b2e43ab0d7b537ab303L - Miller-Rabin test failed.
0x8c13663cc353b90d1d526f372647a27274bcb45bcd1bf1fad0295e5a566a470bL - Miller-Rabin test failed.
0xae5f4656bd2bfe76b7307ddc32c9f04009132e736d823dedc48f93b506164d49L - Miller-Rabin test failed.
0xc5405fb65b4fa12c6e1e1c73f8f774a1f7d45bf26b983d774363329d6ec1753fL - Miller-Rabin test failed.
0xc5cfa2684180d550f5909bf3c46a2fbc298a52cf8ef5108bf561dc65bf3e521bL - Miller-Rabin test failed.
0xf26060072a68dfd044a7a67f7b2867aab2504bb9ab53ec0e9b75f73609431191L - Miller-Rabin test failed.
0xf9681f69d04422a0201a89f60776465594773ebcf5e1cea2d69d8043a26565e5L - Miller-Rabin test failed.
0x96379995f0a8b69912a304b0352845dcee68ae158806f5a10a90a7d167469c41L - Miller-Rabin test failed.
0xc978149f577db8d313f3788b0cdcaef731bf8f101328eef06743337405de9e7L - Miller-Rabin test failed.
0xb7a8ce06133314e42551cb42649a32458e85367bfbefb1a39705a51e88c8f4bL - Miller-Rabin test failed.
0x97546a53fb1d78aaaaccd0ce28e49e24dac76c8473c3c38519d3feedb6f03a6fL - Miller-Rabin test failed.
0xa38180350399ca56ac31aea5894a027bd53e4cd2e24f4015cbf396a0b7f246fdL - Miller-Rabin test failed.
0xec9c9bdb1591b6c818f0e646710895d091016d9e4a8c7350eb3b7de9c8836767L - Miller-Rabin test failed.
0x8a5e3f307afe083b5f174f530593a01bcecdfd256908fb2ce10c5213bcc455b7L - Miller-Rabin test failed.
0xe55395fcb869b71f8e05bdf078ddb7b5c5453785dcf33bc32aebc9dfca15fb35L - Miller-Rabin test failed.
0xa92005a4893ae8f2fb1aa61a3beb7d8c9dbf97d2f816560c187eedc719742a2fL - Miller-Rabin test failed.
0xaa6583e7cb6be2652bdc10ad0a5c3f8ce5f1cb073e35718bae45e13d9db005f1L - Miller-Rabin test failed.
0xb915e5f2498e178853753dc2742664ec5b16e8b3fb0b28f8539ee29247dd386dL - Miller-Rabin test failed.
0xf506328b2020d4cf8c303b6fa2bb2f376ed8ec4097f698d03305f8dc70aca9fdL - Miller-Rabin test failed.
0xc2a3562b436dc9ce12c70fa651dbfd326711ed269530ea2bd121169de106e5dfL - Miller-Rabin test failed.
0xe38729e1b05f28b0648a43ea8edfd3a75517a7941bfb7efba28fd372f06d57dL - Miller-Rabin test failed.
0x8a3d2828a2534add29581916f98ebc5f648d2a85ba88f579e412b8b6f1edc667L - Miller-Rabin test failed.
0xdb244390376b659448f8ec4aa9cfe6f725196ec4902f0a2fbf91c1bd90977b61L - Miller-Rabin test failed.
0xf3f80207a6a8e42d548124dd60c1933182c4b72106e8ece87d2fb4485e81a1e1L - Miller-Rabin test failed.
0xcf47758ebb3485cb2fd9882a26a1e7e722dcada3f686e04a96871d0e9dd34671L - Miller-Rabin test failed.
0xdf60a2f55d1042f6701372fc00ae5d264e43fb0b097cb480a6e2dff0fee6683L - Miller-Rabin test failed.
0xdc71497a7de177fbc3d5ed72fe5618d91a46515b8c6b623a9d6e8b2ce85a6d7L - Miller-Rabin test failed.
0x9ed3c600d7d74ee88a079d590a64f7cbbd7888e8bda322f07165239ebe4d2747L - Miller-Rabin test failed.
0x8d80a9aed164e3895119c6e2c9d23e268ef734136856ac79a303de0409d7d7cdL - Miller-Rabin test failed.
0x9b11d3b6f3c7e3df9ec041b18312fd93f0b4042c6c69156e0d6d49d025656e5bL - Miller-Rabin test failed.
0xfaec9dde3ff941ca1a9640d84e2b03f6204a60f4090a67515e9fefbd00ebbe67L - Miller-Rabin test failed.
0xe3210931f794e4e5c1ab974700aea8fe32bf2526ffe3152062f7204ee2a38163L - Miller-Rabin test failed.
0xab47a1011fe819b5811952dade903b8c995e97a834335a0bb99d197d426bda85L - Miller-Rabin test failed.
0xdde94ac796dd3edf113769f86ee2d1bb6dbb66a2eb47a05ee21ccb2ffe0cb617L - Miller-Rabin test failed.
0xfc069fa1fd414b83f4a4ab4eb41caf039ea4f9c45aeeb584dd81043f2978ef01L - Miller-Rabin test failed.
0xc62d5d784f365b6a0d36de0abfa719fcd519f835873837c970b433044d66f9b9L - Miller-Rabin test failed.
0x87373314bbffc886675218b05190a5e69e92f9d259f8e8d12af6bca3fd0acc59L - Miller-Rabin test failed.
0xf0a56c0d00a31a8a4e2e463b1140c768cfe0044686e65855cace606061432381L - Miller-Rabin test failed.

0xb177f4db67fe975a231a69fd211eb7e0aae441af6c9e1064d625821ddc17c6e5L - Miller-Rabin test failed.
0x97a7ed7fe49fb15f31fe3983d987f741e286fa6c46e5df5ceb851512f713f739L - Miller-Rabin test failed.
0xe7c1915006f9e4165fe1e4690d5c24afecaf37498684c0ce3d0286dfdf5a24afL - Miller-Rabin test failed.
0x9b1286eefb111b576510e1a7b8b631392a226d1204495d913ee669d2a9380801L - Miller-Rabin test failed.
0x99e9a7a4025ff3521a10a32c91fa549844539248b70d2ec3d0bcc235109e80c7L - Miller-Rabin test failed.
0xa993da3f6d51bfca30e87ba40fffb144e77de36eadc4d4509594330ad50e28c61L - Miller-Rabin test failed.
0xe9ab38f54508fa252a6dbaf7ec9706595a22ee49221a6b0a7fc2c6f8e8dbe08fL - Miller-Rabin test failed.
0x9d0f0ca04a8671a2f920c64a02a1ef75b8c1c66ef8d400245dae35bb43c3cf2dL - Miller-Rabin test failed.
0x8dd1e031abe35e38caaad85fcddee6a19dacc83f389832f2bfe9c3adf4e67daa3L - Miller-Rabin test failed.
0xb1649d6caf066bea029f55138d19fce05a1bfa2a3d6799e2f6574ef6c19f6be7L - Miller-Rabin test failed.
0xc4e775ac7290a9d5b3691c7eda31265d433026dac53a643bcf7934375b210dbfL - Miller-Rabin test failed.
0xa8cf725742e2f9c1a03704f895bfd8dfc50bd1eaffc5097f544100b3998f5d11L - Miller-Rabin test failed.
0xcdf7f77d13d93269a7e2e8b0f36341df0108d7f47625849e9df7381fcc9e3ba5L - Miller-Rabin test failed.
0xd064a13b1d1204961b08794f785568aefc08f4131ccadfff9d20ef1702ea677bL - Miller-Rabin test failed.
0xb32daf0ec36afac8489be5c5468827a0c62f1828a05c88c4464ebe3f291432f3L - Miller-Rabin test failed.
0x85427d95878ec91d74ff30d867cb2ec357538d326b92825926a15d6495c0eac3L - Miller-Rabin test failed.
0x9927cd4b0f8cabf9bb8a82a851d25e1b83177d379eb0f10dcac1b37199c45fffl - Miller-Rabin test failed.
0xb3c6e082b8883b4db9567765d88e01e83111cc39d88fc0ec71fece2c26675d5bL - Miller-Rabin test failed.
0xfe44f7f43853479274457e7024416758dea40c9c87516c31d586d80b1071122bL - Miller-Rabin test failed.
0x83f082d95803fc31afc451cbada1087a265058d05928136210aabc2c3682bbc3L - Miller-Rabin test failed.
0xdb71edf786148d6051ee74579aac4d13b5666e01030339d293c4950b40a50023L - Miller-Rabin test failed.
0xd8c8eeb76cd0dc1e03d810869d6c985c5b1e1434e90b9f958e5d14d420b4a0fbL - Miller-Rabin test failed.
0x8bdc8a8a5a396e083823b0ac7cb291902b4f4ada06f55daa74f54ba89354df2fL - Miller-Rabin test failed.
0xd3f857516606f0a705c78b28a3abebfe7dec99fd1db559f39fdeb39048324a3L - Miller-Rabin test failed.
0xdf4456ea43c166fb31d078df3a497336c9c09912e5b63c32abd8f201003728bdL - Miller-Rabin test failed.
0xc74ef5be86452589f66b6825e7240c948d635cf71395bc6395b23a24dc70f0f3L - Miller-Rabin test failed.
0xe8eab5c161cd12c570c2f3a552c0b1ef49693efba1b06f546f3e32f49a0e8681L - Miller-Rabin test failed.
0xae3c68b27b3edc8b1b5bce8b0e6d7679d2c875cb04edc386fa9bb54cb9b4a197L - Miller-Rabin test failed.
0xfad60c89f36700f84d4e56b613b4757d14d6d5e1b86409258951d47656e7e0f1L - Miller-Rabin test failed.
0x88c48f7b5858cea66beda53426305b17e79f32d677ef2eaf3648468e5150a92bL - Miller-Rabin test failed.
0xe9d4d3de9f8122000f451556551f00a9d4b6438f3f9b8b3597116823777e69cdL - Miller-Rabin test failed.
0xb92c59bf4ee7dced52513cf9d56e1bbbed3afa6cb3be1eeb0854f6d58c8f96775L - Miller-Rabin test failed.
0x8a182932064c60aaf20cb1dbfebea905c3d8814b957f8f97724f02533a48cbc3L - Miller-Rabin test failed.
0x9fb7bfad0032e1a86e933f91bfec2cd20cc85135fe1c616ad959f1c36607637fL - Miller-Rabin test failed.
0xb8e39282a52a2793b108b7edef58971e0511a7d05ac89a227fbc68099461e31L - Miller-Rabin test failed.
0xe361b8419697f1eea3867f2ed56e41721b65c2172c4f489896d0f6fcc8301b93L - Miller-Rabin test failed.
0xf6c43726e94cc8a52b2e2f8114a967139f42418bc2231ecdfe7c5d26e9a5ceb7L - Miller-Rabin test failed.
0x8a11056c20923b2b7f5e31bd351a36d93624c447ec91a35a391d248f42470767L - Miller-Rabin test failed.
0xbb0e0743c25491da6a10dd2b4ba83d5d3eaf621807755ce430b83a9628d89869L - Miller-Rabin test failed.
0xa9e61cc31203d3859d60f4e190bb3773e33109ce561499e4bd59d75fced8005L - Miller-Rabin test failed.
0xb0b268931c96842292c975f369d44a2537912f2e83a29cb9e4f59511bfe96b49L - Miller-Rabin test failed.
0xb286da4dde2466ea1aea4aec5ac161abc5793df5e3403bef64268cb4f4c8481L - Miller-Rabin test failed.
0xde9a27af7a26998e33bea2174797e78dc83858091dea4969a72fea80ba263369L - Miller-Rabin test failed.
0x948fd8be3220d4481f07cc826533b856b37a6cb4c87ec2cfa2f2c95de18655ebL - Miller-Rabin test failed.
0x8f277840296762a6c5f2516e0c84c0131e9d1ef04d245f78b44bbbed6f9d8b9b3L - Miller-Rabin test failed.
0x9b5a57d4c3f7ee79903bd2588200980df9aa53264277382cfcb0b35bcfddedd51L - Miller-Rabin test failed.
0xa86dc47afdf56674dd2c504b66267bfc9cf5583cddbdcf91ef799ccf5fc2f4849L - Miller-Rabin test failed.
0x94e21744af69dbaf79ecb4a5a53edb331954ee15f1f81313911988bc31fe9b41L - Miller-Rabin test failed.
0xd317b5ccfc24f8602ff2cf74cc61538ea6c101c3446547866eb644f763664b17L - Miller-Rabin test failed.
0xf4e3554fa6ba2154d15b223efd73c42f4023f95915b27e03407294ca86912515L - Miller-Rabin test failed.
0xdbe0da9192b86821f8ca252da633c9093ac8094916b54a57c4d7cc2a88434d99L - Miller-Rabin test failed.
0xe6c87f50e949085262680550cce94c4612685f904ef1af22b8e4b9d544303a3dL - Miller-Rabin test failed.
0xacc550e8effe100b5c30270c65ea5acdb8456fba32b464da34206a2b158479b1L - Miller-Rabin test failed.
0x90cbce342e72f01f255d18e18aafea794e7b330c3bed8e4f996501574e90ced7L - Miller-Rabin test failed.
0xf895dde0f92ce54b47e4b1b97875305b205463163a868ee1dc734698ee2e2667L - Miller-Rabin test failed.
0xf17b1b3ab517e44ff6114f76d60e9b8f1730a44300bdf25e8803798d4bb7cd49L - Miller-Rabin test failed.
0x88417bbca0a36f62713d508529785af6b2b41f76c6d6c9e68e7723aeb5cf9ff7L - Miller-Rabin test failed.
0xcbeb376473460d58c6a853193a525d1c14c4ca3e636bbc8a511bd8cdf06b1685L - Miller-Rabin test failed.

0x9b228c47d4bdda0f583d075107feb5e7482cdd2f7e944b43f56e737b91e25bd1L - Miller-Rabin test failed.
0xa982c72dbdcfcb1308177ab85b40dcfa565a5e9bf7e6eb34a28146f0e4231459L - Miller-Rabin test failed.
0xf78d7798a4f56b1bf639681b09ae53aa45b074ba2db343de2810bd378dbfba9dL - Miller-Rabin test failed.
0xfc1299d7d05e3c901f7cb1633318b10498e0fbaff1a159314a43380308c6cb5L - Miller-Rabin test failed.
0x8f78d623f38f2d7717e536ac1f2ae9f68bbbcd7dc326daacb3d3cf524bc77d55L - Miller-Rabin test failed.
0xbc1e05ac1b5a525745e5467e7423ab886824f4dcabe4eb01409af4a1865a823fL - Miller-Rabin test failed.
0xb1cc333892cfb9a06321d96cdfd11275eb557e34a8d04109a1e336ef60f25c01L - Miller-Rabin test failed.
0xc28e884ed245699d26ca60f665eebefc43a17220ed4dc8975ae61399f9a1de57L - Miller-Rabin test failed.
0xe49e1f9cacb895a4d1f1f2796f46930946e3b08d2f6c8d567b2d25bd1e5c8165L - Miller-Rabin test failed.
0x9504a38546dbe8db0cc3dbbd7640d788023a2d8df253cafe4e436cb59ecef779L - Miller-Rabin test failed.
0x80aa4dd457805578f78e305116b1db9c77f30091405a3eec822456e08c4f401dL - Miller-Rabin test failed.
0xb7e58a00af23968071b513664433b9a44037eb453a80a321d09ad728e1964bb9L - Miller-Rabin test failed.
0xea3485021be282676f3f613ac7ed03be14e9105f1c8c842868bc9420ccdb38fdL - Miller-Rabin test failed.
0xe32fccab1b0a368d42b4465c8c97bda84595fc4b3208d45dceedcba9daf10a8bdL - Miller-Rabin test failed.
0x894f3e05f498dbbf685a74a416cb93fc6acbd7f8b9c6f5aa4ac2a53258465a03L - Miller-Rabin test failed.
0x8f95f90b727bf1be6e3d22c3fe7f8c22d55c0e03698a3e43f1618fd81943f949L - Miller-Rabin test failed.
0xa1c2f8f79dcdd5851b1c1236b734627dd885d26deaf5063fefeb94cde0b9c1e1L - Miller-Rabin test failed.
0xe1addf3558d42b6211ee3952b1433430f24e05340b95caaa9e4e01dd10419f9bL - Miller-Rabin test failed.
0xb94e3053f27e28317bf5f501409718c3c873ccf9dc8df387677cd0ba4598a165L - Miller-Rabin test failed.
0xc18d4e13a3899b998b72ea42b96c4592f8bbbeb592a5c7b2dd980442d1c75f26dL - Miller-Rabin test failed.
0xfa5c214850f7380ca307cdcc269c585c4c7c61210fbbcef04e6fe699ea439e21L - Miller-Rabin test failed.
0x88aba6a49401d62cb778087df921de791d92f9f042372ba63cec667da5072893L - Miller-Rabin test failed.
0xa9d4535d17b4dbcb42a597e05b47be53aaefccaa79b6b5381e08d2ac7503141L - Miller-Rabin test failed.
0xa09b38f712a24807aa0bb66ead2c2c083008a0536b3586855f39915a95c70d87L - Miller-Rabin test failed.
0xca254d6e22bced32212ee8b787ab566910b35100335fc11789dbd1431352cb07L - Miller-Rabin test failed.
0x85ee191fe0ed293c8c43c75ead334bb25ceb26b0a27baac1ad808a92126c5a31L - Miller-Rabin test failed.
0xd2bfbecb7f66523b9f3356a7615f89825b027c30d0a8fb3e904ab1ea674b3aa3L - Miller-Rabin test failed.
0xae5d8618dcaa0f6b0b24e28ab1eb638c8461fe9aafaab2b2e36d4915bf101183L - Miller-Rabin test failed.
0xe6d4e002c7cd0d0bda9993f724f30c2f35f27a8844a8bc6a98e21fdb01919dabL - Miller-Rabin test failed.
0xe4e337f68e44810365766b21393cc1040f5038ec6bbdcafcf659fe21bc12129bL - Miller-Rabin test failed.
0x9e05f453a34326e72c38f8cae08f1fab08d7175ae86e9602391d3a77b95b967dL - Miller-Rabin test failed.
0x811e4a670c8fee9db18033a886a8ccbc24cbf90281b5a29eb019da4b2a7c917bL - Miller-Rabin test failed.
0xe54dbb7e554e871d3133a478f32a88799bc2c74b07ed53f32ab61159be69159fL - Miller-Rabin test failed.
0xafaf77a032ffdbf747e0b1f8f9cf8326c61e1d9a3bf9acea8b644bf1fbfec6e3L - Miller-Rabin test failed.
0x8928e6de21cca24e0578e64b05a36f6513f49315c9b4b20fbb3ff848a3f1829bL - Miller-Rabin test failed.
0x8484bbbd4a62adc386fb7b40ea4c6c1d208f4186e03ea6b7bf6525c8e17d3d61L - Miller-Rabin test failed.
0xba756d8278d62eb69daf0f577c1fc0cb45c6916520b1d0cc553c07c88ddf4111L - Miller-Rabin test failed.
0xd9fecb5a70a96909dd98d5fb24e0e68bd6cd7abe5081bd5768defdac749560dL - Miller-Rabin test failed.
0x82d886c66a2c5e227e522e832b246c5fd3c06d22eaf3c699c5e6659b74e73fafL - Miller-Rabin test failed.
0xbfde8c182accba21127580993f87fbb36ca87fa5c44df0d2b05f3fa40995ea9bL - Miller-Rabin test failed.
0x9b06fa86eb450ff70297495d19639a188896dcd26efd684b290e2dd9434bb069L - Miller-Rabin test failed.
0xc00869c463a459325c02d13d147100fdb7a46e0c206db38d89d79daca895743L - Miller-Rabin test failed.
0x80faff5b75e995e3cfffcae703f043a7fbc5cc51b58af52e5a2be486d4aa7d33L - Miller-Rabin test passed.
0xeb004b675f7998a3c5dda8b9c4ac15543368ab2b29249d81bad9aceca4fe341dL - Miller-Rabin test failed.
0xe0b75771115e61ca9a95dbb2762825600327ed9fb71a3c265ee6a5651b24a531L - Miller-Rabin test failed.
0x8e6dfd8d82634417dc544aa35a69992570dbc24809366f8afa48122e573e4439L - Miller-Rabin test failed.
0xef5ddedc7264e9317e0acbb306547e96881ac758a07485e48b1049cb4ee7e3cdL - Miller-Rabin test failed.
0xf33e6a6f63e17b526d4ac941c53d56cccfe1f89248f2d96a942b0fa1a4709fedL - Miller-Rabin test failed.
0xb3aaabfbfc0768174ec5cbc1825e4a09d03503b88d62f1133a4e269f62f79b123L - Miller-Rabin test failed.
0x99727e9b7d125d42a747c83f40f60347d415304e4b87be7de7f645b0f6e61727L - Miller-Rabin test failed.
0xe2a6eacab09d1fd9da45f819f49ac6521fa9a7c4d4d2027f378368f3c6771fe9L - Miller-Rabin test failed.
0xd24eacec9f629bf34e4f61677ee2b7518c0f4e71e577e9b517f38f0728632649L - Miller-Rabin test failed.
0x81f19931fe7eb6e468e550ecd2f2f765b5f26ce719627b88edcb304f5804d48bL - Miller-Rabin test failed.
0xa95dc3e707a96f3e9fcfec99a7130fc63cd0f60e09a37247bcad824ff5698229L - Miller-Rabin test failed.
0xcxa3231a5bb3f05d4e927c7356ee5b2e03ce629d6891c69e69d2796bc47e35cdL - Miller-Rabin test failed.
0xae218e6fd36c581d3b9029127b3b1c7a4477dc4024ba031e26b5d4693f61b035L - Miller-Rabin test failed.
0x8b9ee174d3389bd025f0a4e9c98fe5650c4f63ce999877a520df431957e46dfbL - Miller-Rabin test failed.
0xd2ab5a4d33057cf6aa8b6fe9fbc9ab97f1aced718e5f14a6c550438f719ff71L - Miller-Rabin test failed.

0xfa85d7053dcd544de5d1c490642a49621ab144817fabf1c19ee155de28eb54b1L - Miller-Rabin test failed.
0xb4eba3c2bf9af2503f106f5d45312c51b05c068694c55fe4f5d6688726e12e41L - Miller-Rabin test failed.
0xf105788494455a5b17b1729acf48f2de6943f719321a112592e7e117864f39a7L - Miller-Rabin test failed.
0xce084e2416b0ae822fceb212000df00c6c0079c1441803ba61346f7875f0ee3L - Miller-Rabin test failed.
0xe66a7544cfb4a4ebbc9f7971bec574d7a999736d512a88b97fba6d758ef3f8b7L - Miller-Rabin test passed.
0xa49955fd6312db234bc848a009ea2715086941c6f471baad07a763f2fa4925b5L - Miller-Rabin test failed.
0xeb9b01916b58b04bb25682378504930177a64a5958d4b855eb3fea1292226a6bL - Miller-Rabin test failed.
0xf323c12a839013e47bfd64e2f31ab752d72d59f75f8eea82b20f374fb7184f85L - Miller-Rabin test failed.
0x89cac0f5033d769cd05b308a139b1e2fb870ec41174ab143c12bc0186869e70fL - Miller-Rabin test failed.
0x85053964164935adb8fab7d20bf10307ee94aeaefd6074820f2d8ccfba069831L - Miller-Rabin test failed.
0xad0e405fbc15e7ed7af10821fac3c126dae105a5def78749ee019929088dbc77L - Miller-Rabin test failed.
0xd82078f3ded62cbd41ded0f7a4cd1a1b1d1d71e095ad217355dd34d0a81e8965L - Miller-Rabin test failed.
0xe99c41aa1e8fe6dc061a1963c4ac1b69ca5038e0a4f3f3a887ee70cb1cbaaf4bL - Miller-Rabin test failed.
0xb619e3f17bb0ebe876a7e5d83c31bae75dab98b8027d102cd887e5c3924cb529L - Miller-Rabin test failed.
0x90969de5de827f02daa623814967bfb7d0e495162a57530233f44bad4c510441L - Miller-Rabin test failed.
0xf4d0c2064ce0bac54f8cf2bfa4bde48c15fbcf225286459dc47599b51f1f190dL - Miller-Rabin test failed.
0xd674324993d0c9ed083d2a36568f1204c3c00a7057da065a723ab43cdfb544cfL - Miller-Rabin test failed.
0x8a010442c8407eb5590c6ae956054921971d82b68f0ca749878cc50efd10b417L - Miller-Rabin test failed.
0xcbfa4f113f10ba78443dc1bd20cb4640a660f105e721a6a3c357fe694146402bL - Miller-Rabin test failed.
0xe5d292f61bff5c543254bc78e182ca368e9edba05aca355475435af2607a9485L - Miller-Rabin test failed.
0xb216d980f8528de0ee900092bd37d22b7f4281dd7dac3c6fac46f21cb64c69a3L - Miller-Rabin test failed.
0xb656e7fd338f7a7ee4b5c7c763d60c04fa26e370bf88731b9ee2e319c55f25b3L - Miller-Rabin test failed.
0x8408cc038d5039b8752c4ab4414193e870f0d29a3fe5418a768023daf3192379L - Miller-Rabin test failed.
0x8de86dbf922ce4afeb16b95d3f3afa5f31cc04cf272f3dbad1fff4724c70397bL - Miller-Rabin test failed.
0x8febfccfcce0d77eaf1eeeadcf86123a163a95dedd7d57c9fc64b4c1ec5281fL - Miller-Rabin test failed.
0xd56d322afc90af9644e1cc8868d00bbf589ae42f256e769f5ad0f2eeaac366ebL - Miller-Rabin test failed.
0x9a3e8902a848be31f43b985431cd32c3a521c1b4575b18e7f61e0be72930a6d1L - Miller-Rabin test failed.
0x984eac9cb263e717ea5b90d2bf8c110ead50a865f8cc20bbd402c0778550455bL - Miller-Rabin test failed.
0x8d4b4b6fa29fadba4837db8424dc6d7a7ea7853332290cef1af0b0ec17032019L - Miller-Rabin test failed.
0xbfeff8c06ba42c2b814f82a840ff3d0c2f4e247f638383b900535c30fc06f10e9L - Miller-Rabin test failed.
0xccd3f84b05defd0843cf91c0d65d236e25149c527450a5890df06e0b823a2cf7L - Miller-Rabin test failed.
0x88597b308ab3476bc9352ac2d69f4e31b052b39a1a0a9047e193b7f3a9854febL - Miller-Rabin test failed.
0xdd9751e90f4ca7df8e6f1c2ae959f9ca5741a28815510889003651b84771291L - Miller-Rabin test failed.
0xf75b97a9f9aac84f35d7f41731c3e02ad4a281d55f690654440b4564d620ac47L - Miller-Rabin test failed.
0xff1898940f2fb230b6d51a3f4d0729db8f2a0b20f0264d95717d8d1a2784c7bfL - Miller-Rabin test failed.
0xf6851177d071266c24e15e8d261f7a64eec8c31996478fe5eb616c66ff2935d9L - Miller-Rabin test failed.
0xfe18754817bcf1aa0c8d1928a6e66813c378141d597780c80474b6c67971e3e5L - Miller-Rabin test failed.
0xb92b4a9dec86628fe7238759369f15d65c6721817b97036c181cb1fd2cb6d4adL - Miller-Rabin test failed.
0xceaa864dc8e1527ae5f318d2bad8a66d7b9bd0826d76ca7cf9cfc633774a90ddL - Miller-Rabin test failed.
0x89342fdb1b32ed719d82a811cf3e0aa2ad486fd5682f7d43a37f4ded25ba815L - Miller-Rabin test failed.
0xb6f4e2990428992e648aeaa4d3715e0abdc98d64c4c633bcb0c3d6366c3436cfL - Miller-Rabin test failed.
0x9b031c03c7ef3de7937fa78d053e21ec501e54837a462333dd4719d49b4231cdL - Miller-Rabin test failed.
0xca52be61c695e1c1de800f37dd26f73efa7fad859dc631a48790a8e3415b5ccbL - Miller-Rabin test failed.
0xcd3cd19187c6c18dfc3d828c569a4eeb925106bb27790b736eb88fc516ce086bL - Miller-Rabin test failed.
0x961f88f9a057fba422d44b04ac1265fba2117dcda066b867d0213b764cac530bL - Miller-Rabin test failed.
0xbe50f0650600c66d9eb61d5bd30dc346552be76d83c46fd0cdca05d6ceacdb55L - Miller-Rabin test failed.
0xfae96ced33b1f66ecf76bc27768fb99e3bd1e74cc87627489031612b296c87fbL - Miller-Rabin test failed.
0x91a524d4bdc518afc01da5a382cda4cced4e20f2aaf1c1d9e537fcdd137a1933L - Miller-Rabin test failed.
0xe410bef4695401da71f158cc46d5bd927d6644e7f10c8d73535d41d6ae3f10d9L - Miller-Rabin test failed.
0xe0192918ee050fcc7304a11dc57e10327d08dbe66b253b2644d192989086d19dL - Miller-Rabin test failed.
0xe9f3eab2ff115897b20d817425d5c8291042139523c56342859587465c5bdb9L - Miller-Rabin test failed.
0xe3e4e4c6961c1ef8b186fc9fa82a3abd644b8cedfb0aaeb1d4df764f5ce77c5L - Miller-Rabin test failed.
0x9480be082d0b973dea7829bbaa5ab3aff0c8114a0a9f1374ec3ee74662eaf1bL - Miller-Rabin test failed.
0x872a4371425297062699390356dbd666b6881d68e0b209e6d502da1e33a0cdc7L - Miller-Rabin test failed.
0xd4465a09020bc13993d086f579714d05e147b4465c5cb7dabe23df1d64219b2dL - Miller-Rabin test failed.
0xe859432513e06e419bdb9940f96d9b20cf323f7cb40c3cc2693b6326cd00a9d5L - Miller-Rabin test failed.
0xf37322a479fc90b82d06b2d075fe7aea95fab7c1577a95519f06989dc204297L - Miller-Rabin test failed.
0xb9770f89d1998ceae757092c12eda57151ed79041adba7588763a9179a8b4717L - Miller-Rabin test failed.

0xcd27940a4cb655b7f7878165599cee67661d9f8cf3673a39c8ad251df82a2185L - Miller-Rabin test failed.
0xff5d80eb9ca1e1afaff53cc535ae099910fa5b33504ea466de6d6626d3af8f8bL - Miller-Rabin test failed.
0x9f6b02abf1d1fc966663fd129e91fabe96306e7ceee63ed2c3865206334665abL - Miller-Rabin test failed.
0xce46fee892b4e768fa00bdf1f7bdafe3dc3327da71048c95ce3d1d344291c7L - Miller-Rabin test failed.
0xb7553db520d105c0e521d1f040dac6cebe719be7e9d1f9799187c9debb755ec3L - Miller-Rabin test failed.
0xfcca7b60a77ca88c6e35fd07a65f5093d456a7fc81dc1239b5702f438817e15bL - Miller-Rabin test failed.
0xa049694ae94b41efd5d08772e342e4dc04b546b8086201f52c5622bfc003ad1bL - Miller-Rabin test failed.
0xf5918993bdfac78b977a0fad14a8b94f8b5ee0a2544cc92368c3236b90abbedfL - Miller-Rabin test failed.
0xacea9482e325e6372fd0d80782b4cee9193a640702808894cda6aebecf4304dL - Miller-Rabin test failed.
0xd210d86123c0c7a55b4a2e8fe0fe7b7948ebfb970cf560cd6103e7c18e0263c3L - Miller-Rabin test failed.
0xc6ebe1a83a3720bdd090b5e22bdc704d87fdb653f1d65f8e55738ae5af03c351L - Miller-Rabin test failed.
0xa544926fd85c8f8ab2835b70a7c09c0607c05e2e00959b140df924b55e5fa55bL - Miller-Rabin test failed.
0xe88fd02e325fa14cc845ac20722979a2695a95d26e60608a364a9d5ab878a785L - Miller-Rabin test failed.
0xdc1bb3c5a011dd3dde08b4e95c32deb4cfa719825e9e6e7a64e98a5e3cee3abL - Miller-Rabin test failed.
0x9cd2622567ab3eb6f3dab8b0ccdf0410eccd9ffbc4e46aa8efde9883ec1b0241L - Miller-Rabin test failed.
0x8b4e79f576e8f1d41726c20c466cac7782d10b05c8e54c0e1a01ef82211da33dL - Miller-Rabin test failed.
0x9b1ff98bc4cc857d33465ee2365eb0eb1469551bc111bbbbbcaacadc8e9c85e1L - Miller-Rabin test failed.
0xd3afbaf32d17f43b568b0ffa66870ff1b58bc70402226c6f3e8198e200cd6875L - Miller-Rabin test failed.
0xc75cd466fa0dc622edc62abc2172429f79ad6f6a6390687b06894cd09407ebb5L - Miller-Rabin test failed.
0xfc67610f60b60fd3e76014bf3b8686a15a9230bff3389e951f177e10d8839b7L - Miller-Rabin test failed.
0xeab05897af3d32237ceaaeb2ef6e00921a0fed627a98ab8d2137245bddd8be15L - Miller-Rabin test failed.
0xf4ba1385230636aee27b2f660949ef101ace6592c3e60a1d7e2e5c9d9b70f31L - Miller-Rabin test failed.
0xce4905420c933781918bb4bb99588c4927e550ee0c1a782803e106f1a7692241L - Miller-Rabin test failed.
0xb7014527ce4c5ee72e4d757ddb1152ba6a8db90a9f8d41aae71a5ea30b680b3L - Miller-Rabin test failed.
0x9d08564ac85a0bae293aaf3ebc150e2eb75f1aa9b14fc5f908ebc68a489e3217L - Miller-Rabin test failed.
0xb8a23275071a06ea2b0ad98b5de54a826b7471e5307917fa70bede580057b6b3L - Miller-Rabin test failed.
0xc2d8afa51d73f7ebcc87915d0c7522547b9d3bf49703d8452e71b4511e0acec5L - Miller-Rabin test failed.
0xde19ff338d8a6a53c621bd324b89e4adc1c308968d4201e791b023fbd0b9a759L - Miller-Rabin test failed.
0xa2c20e74bbf922de560dbdd09a104c84ecb08100f3ea8e49bb41355a3d6b7a8fL - Miller-Rabin test failed.
0x8c5ae2ea893d296584046a77e2f9b773d541e6057962f30644406afd737672b5L - Miller-Rabin test failed.
0x9aa8e403ed6f016a534cbe026022c2ed77858f9812eebecf49b5803660383ecdL - Miller-Rabin test failed.
0xae9c4e8e1a759d4b4c4cdf97989d68f542dff05518045bc2fc522be98c60bda5L - Miller-Rabin test failed.
0xd1485d7b2a29fd6697648cfe8baa1f7818102d0762fcaa9de263933f63a5f7b9L - Miller-Rabin test failed.
0xd0046fa19d48fb31b52d25fa2c68f7a6a35e93ab5667ad2aacad1b38f9468fc7L - Miller-Rabin test failed.
0x833cc63b5c658fe0923c0e118b7c75c4f7399aa798ecb738c53934f187aaca31L - Miller-Rabin test failed.
0x85cd4c2aad5c0a5da95c62a875d4cb1bb901578950a93361904a494e5268bd85L - Miller-Rabin test failed.
0xd5fdbbeeb120a2312d69e9dfd03b8fb1d70d81b7df938db601edb0969f411acfbL - Miller-Rabin test failed.
0xeef521a047740fb6c0874fe51aa42cb24a19219588512663d4cda36b39152de9L - Miller-Rabin test failed.
0xd27216a839e759a00375bcac6d651c0f032a314f31b5cd1026f4af757fa55ec1L - Miller-Rabin test failed.
0x98d4757a473c512b840bd40d43e7056b436a2aa657cca3fc3c3b1c1793bb0783L - Miller-Rabin test failed.
0xd14e85e799992962db9f3eb86eee1f29491a2702e19909bbe7eee5709a02ea3dL - Miller-Rabin test failed.
0xb499ecc8bd6a5f4ddc365d75fbc9cb75b77319fa8ebf042d494c02f88755e9b3L - Miller-Rabin test failed.
0x9838b44b1c57a2d5c1c50fdaacb3eb09362480508f48abd1b54b19d73dc68271L - Miller-Rabin test failed.
0x9cb8b54727f4cdcb3d69fb45b26c356ae9fadff27ae2f5c72b5bd19c95aec1bL - Miller-Rabin test failed.
0xeab0a2ecdcc9e9e9f6b5988767d7bd285005eb3df009f521308fab398c65ff45L - Miller-Rabin test failed.
0x85264a22d18abd61826d2c3fe25ac9d6677d2bec5955eca7b8857e745e2ee5efL - Miller-Rabin test failed.
0x9992879e33c883bdbcd64ba4e0458d6ca70fab53d628d85975d922e75fdc8ea9L - Miller-Rabin test failed.
0xf24fc9d89f2a170bed2503b0fda0091eb43a334ef86b075877526f50ca9d2d1dL - Miller-Rabin test failed.
0xbd395bdd363df996db954663dc2a5dbd84dcaa1feda411ed9903e6c7b59d4459L - Miller-Rabin test failed.
0xff902ca7322b25d0f232a48087b51c30be1386a2bc6be60025d6f60117c3de3bL - Miller-Rabin test failed.
0xe47bddd50c50e2302d8ca44a749b6ffdddc761ac9f64314ca178ec5539028bebL - Miller-Rabin test failed.
0x9865d2c6ade61b603ce2bc8a89d4e20929306f1709cd55680a6fb06f5822abc3L - Miller-Rabin test failed.
0xe12786958af4db0f2235bbf45077c9a8f61ad71ab71aad04caf3238b2f1ca051L - Miller-Rabin test failed.
0xf5dee80f3a583ff4c246bf85221eb764d97f3fb848a5ced90fa8859a58fe4c07L - Miller-Rabin test failed.
0xb5ed5909a65affc2057dc374a254b671ccc71c6c205e0906f49b38f5bd156a15L - Miller-Rabin test failed.
0xb577b135f6d2ef01ac3e4052cf8bddb575aa322fabd3ca1499f85ef6fc96beebL - Miller-Rabin test failed.
0xa9205e7b0d6ce88fd5f6f7ab4753a4007847d13a9e7eb4c3ecd50ba38f06b58dL - Miller-Rabin test failed.
0xd515d242833124df93f8dd8dfef0487389905e020a527860e33a32e0ab4fe7d9L - Miller-Rabin test failed.

0xb1306000526b43c5a09d19b896c0c6beaf9ade36cd1501833a1530c40bdba577L - Miller-Rabin test failed.
0xe67b84d873fc0b698b233da153d9b6259daec8a79b8f10563dde80c131dc8219L - Miller-Rabin test failed.
0xbac7e5ca1109e5b14f660ee10b472824418469956a06a95967600d2367487e7dL - Miller-Rabin test failed.
0xd2e71a7456821b8403c4a360a536bb33725be799dec8455f5c3a10c5d69d8f7L - Miller-Rabin test failed.
0x852e9a12d0b69e689018824d5b2054d54acdcef3dc12d39c66c81b77a9025529L - Miller-Rabin test failed.
0xf5e8bef0705745af6b124e73ab165125e426d1c101bec67b54248bec09e9d6c1L - Miller-Rabin test failed.
0xb071df755e7dab44b265b42d4ba5b8c477e0d28d0d68e640a897edcdb93cd3f5L - Miller-Rabin test failed.
0x8f9c4b69e5f8a689364253ec9c99ee31edd59a1188a123c4ec0ad6105384df29L - Miller-Rabin test failed.
0xda95877ac87b6a87f7e67b0700d87e1d54d94f1c70111d5e2ee26267b6a84493L - Miller-Rabin test failed.
0xb4e08f0356a7c100f9b8bf2313c188a38fde913e6de527f4e1277d0c8ca65d2fL - Miller-Rabin test failed.
0xc2362597561d99579f933c737760ece7461423ee38d67efb147b39ad3840f22fL - Miller-Rabin test failed.
0x93950451ea6794fcd6e33ba7e9096590f475002c297b992215b7d8b239129563L - Miller-Rabin test failed.
0xf18e047b20c55f62d1c8780dcb008e7d9158a6b755f969e2a314a22f671c3903L - Miller-Rabin test failed.
0xb87ac21967a0ccf53aa8ecdd67e12ed391c5bd875471d840cad31cee6e45aad1L - Miller-Rabin test failed.
0xf49733c2258599aff2fec1242d33c08227e49d109724fdd6b4ea28631b5b6f09L - Miller-Rabin test failed.
0xaffce5134a4b34f70c303c83050f0e13ce29ae657e47a1f2cb4470a1c9f35fc5L - Miller-Rabin test failed.
0xd546a637f39f13f59376606a608445bcdbbaf31ba2c399835293bc29b66b34d5L - Miller-Rabin test failed.
0xdef1dc817e5fb17c2d9fb6010c82fe6364ddcb3ac2cb23a911045dc74fca9a5fL - Miller-Rabin test failed.
0xd24c209cd87cc70a408366f30e24b2643d0aaa49f00a73cd9217ba8c9606ec45L - Miller-Rabin test failed.
0xa4c67f7e0dcf81cd2dfadf30aee457a2d2e634bc3f2dd1d440bfa77e45ffb11L - Miller-Rabin test failed.
0x92f040c935c723cf946ff38f4b007c147f5cdeb40c0560931471d060fe9b598bL - Miller-Rabin test failed.
0xd4e746e406f7afd8d9acf7e986ec8f203d9e6e319422a173ac1af6b75f6aee2fL - Miller-Rabin test failed.
0xc348e475ec4b731f563fa753ded5325a98e1256d9ceaba6ec74a77955dc8598dL - Miller-Rabin test failed.
0xcf4a29649aab97b0f33f8eb3ed2b048b7ccc3c7bdc3ecc9b6f9f5614ce3f1f6bL - Miller-Rabin test failed.
0xc48d4bd120257242cbe3d7a69ad6a7e9edeb3a7f96efa749c427229f96309a95L - Miller-Rabin test failed.
0xe0f9a6684a67adc7ea29dcea7df66973246a30fb5549935b6f7c137bbc59ca69L - Miller-Rabin test failed.
0xbd0e3871219fb7a9a479c204c437567aeb41aa329a6de364701efb78dde0242bL - Miller-Rabin test failed.
0xd8f66662d413d6c4c462f5d45d8f47fff1946ed02afa7ab96807fff2498f1b9fL - Miller-Rabin test failed.
0xbe41c09e77c33569917048bcf2df8797fb8e52f82db79a463d920d3ba0e21a9dL - Miller-Rabin test failed.
0x94355748ffd2b1308722d765a4428ecaebd7cf0b11d5c0d07a87f90d6ecfc7afL - Miller-Rabin test failed.
0xc271f5b6ce45c6e9ea1c982d53bd7a7d3640abef9c6d393ebc0cf6fc67fda6b1L - Miller-Rabin test failed.
0xafa9bb48f3eb6dbae212a28850ef5065b385dc668aba5597947177640c8f85cdL - Miller-Rabin test failed.
0x958dc6e77fa74e606050db3c3d8d468c8fa8cce393786ebfba65a03c95141cf9L - Miller-Rabin test failed.
0xcc9f0c0abe711d2f6b9bbd314bfaeb3b2dc4e3dc7fc336c61dde6f3e8d99b803L - Miller-Rabin test failed.
0x92730e4c7fb60322a5acc232eb7ec33f9d5fb1c172d638bdba8eb026f619d51bL - Miller-Rabin test failed.
0xa5c2708359596af0a67ca671642cc3c68cbf66ac786a43fec527b685df248d83L - Miller-Rabin test passed.
0x84a68d5566456c4b22a4dd3048ad39c6e1ee897163cccc5e7e29668058e34267L - Miller-Rabin test failed.
0xe868b4a6df6048ac335f0a95e8e83703b82a93e5b5b2e23205523dd44c854715L - Miller-Rabin test failed.
0xd353993f00b2ed80221667fe0e9836ace812d780da42eb4308d1f45e5472c0dfL - Miller-Rabin test failed.
0xab8a1a594dfdc3e5f68173252964f027bff90650227acbde664218c027db70bL - Miller-Rabin test failed.
0xb95cb4a1c3c5daa0b8fab33b933a24155f0979ac1851683bb0fb948c80e93777L - Miller-Rabin test failed.
0xda28baac444c0f11ebc5c4236b8590470e6912fcf03a3d0b2be59e116b31773fL - Miller-Rabin test failed.
0xbe6779d32ae5db4b927a0367d9a64b3b2569c5e06f32e00b0839d3a162abfa27L - Miller-Rabin test failed.
0xaeeeb88b8dc557d6026b82722e069d887aaed1ef241f943004df34aac8654c51L - Miller-Rabin test failed.
0x8ce320fe0b24f08343478153a2af53aa0e2728e7a7d8454f60fea731682a234dL - Miller-Rabin test failed.
0xbd76b95e74587c138b1196e2aabe8c22416ec2b6db323920a18abd41df91dc6fL - Miller-Rabin test failed.
0xc6ba8e7c593d74bd781895cb9fcc65ad4eee0cda67eb0b589162619dfd4721ddL - Miller-Rabin test failed.
0xf2714058eac5aa77cc8d60c17fa846f615c8e6c5f403ecf60c9ce99c4f443d87L - Miller-Rabin test failed.
0xf4d64c2b6d0d8baf5783a712f771d6005742addfb98994547f4ee1d20ccd6583L - Miller-Rabin test failed.
0x8a6f4b837c346228a4d8672525dd40d480d06e0c58db79edb0ba478f8b28d981L - Miller-Rabin test failed.
0xda90d85771570888f25b6fbd00c9896a959237822f3427360ac9f745aa24454bL - Miller-Rabin test failed.
0xf0383715ac469fe64edf54e8df4b9d51ecc70e43c0cf6e07f216cbf9f9c38d89L - Miller-Rabin test failed.
0x9515b4d4c8c3a4887d8450496a26d22b0d62a52b69cf7b8636dad5c9faa511c7L - Miller-Rabin test failed.
0xc8d86a5c1f95246b267ba0243d58e3db8c200151b471c49ebc6165a838aec607L - Miller-Rabin test failed.
0xb394e9fa4965e91cbaaefa6ada01ffa1b85a93158cfb3749d4d868df299e4c2dL - Miller-Rabin test failed.
0x94754234ffad0031ad516ef1106501f2d8fe2800668f21025ddb8751b1763033L - Miller-Rabin test failed.
0x927fe422031bf87ae3be4974851d9d7d97e66c63f4d7fd16d0e29c710f1eb8d5L - Miller-Rabin test failed.
0xac279e4d498922c9af838f9cf0622b83c93e119c39b5302dad68fb1d559249bbL - Miller-Rabin test failed.

0xae26b6dd61b96c16238e6414c02c9990226b68b27a535196bb7be2bf4a8a385bL - Miller-Rabin test failed.
0xc69e5e0afe53cb66e96280cc3e4a44558e8e73a4f89eb1518f080c36544a4c7bL - Miller-Rabin test failed.
0x96beb492d8dbb4aee1d4c69df57a6cc68f948c9c837686d99d9726dfe83941afL - Miller-Rabin test failed.
0xa8b2ec18edbe987f05205aaacfc99c74916196f96e1676487b34e0b03f0fd467L - Miller-Rabin test failed.
0xede720995e00736c5279a72194d7105c734b1c0bfa7635e9e734ac25f62fc777L - Miller-Rabin test failed.
0xbe5d89057152f0c32ec9eb73e5b3512b3d4c71800859f1ec4d779030cf9048fdL - Miller-Rabin test failed.
0x9d09de712371f8e413abdaf42e27dbca893b2d577efc5d3410769a91b2eb87fdL - Miller-Rabin test failed.
0xdfb49db09f3e638ca3dc60f84fd91f8a8aa5b28563186b1948f01ba881cd4a3fL - Miller-Rabin test failed.
0xd5331c64c21f027137f8030f9084f567b88b2b2bc5efccee0074bf2cfb065d5L - Miller-Rabin test failed.
0xd5d6d6ed054a00b65cd37d4dcb8b4b3edae63509af7903b550bd9207946450afL - Miller-Rabin test failed.
0xc3409874904936e8d32d5b59804249a4a16bad22393614fb75c03b969f8aaa65L - Miller-Rabin test failed.
0xaaad6d95929d00cb60c74698df932b1a87485d4e15d6f2baae5b4b1d978fed7bL - Miller-Rabin test failed.
0x9355b53ec70840eca63aa9b133e14a27c570bbadba6557a68d230c42caa9c3e1L - Miller-Rabin test failed.
0xe98ea96c398563d12e7d526baa3d6364673d1402e334b18c8174cb91d1b3291bL - Miller-Rabin test failed.
0xe8aae72fa533837ade91e6e6627a3115a628d6911ddb1e6fd5c5cbc30921b879L - Miller-Rabin test failed.
0xa21102a6748fc1fcd6bf0b3b718c144adb793c45dee5a291a20e791f9602cb8dL - Miller-Rabin test failed.
0xe7eb4b223ec1af8671cd2469266ee06674f1814ac84d03895efb99f85ab4ce55L - Miller-Rabin test failed.
0xe2b8d3ee47e4ad5ff299e018e2d0a0f8c41979ccc8fd7e2ed5d494e39545526bL - Miller-Rabin test failed.
0x8b699a7078002a3601f25bd414b0729b166be1444f0d2f5d0606a8a70c29b8a5L - Miller-Rabin test failed.
0x9c3905073e6b65d29b46ea5aadef8297cfa388a44922eb38d938e4c83ce2d557L - Miller-Rabin test failed.
0xdb0386a2a1a9a2b7b4d019da0924ea78259a2ba1b6270c6b2035831766ae81cbL - Miller-Rabin test failed.
0xa04ba7c2ed84bb94faa873cee9fcaa634437ac455472353cf6b4fa466ca4fc05L - Miller-Rabin test failed.
0x925a148ae1ee0b55d30136af65e39acca6c2facbd68361a011d45192a6f6890dL - Miller-Rabin test failed.
0xd9fe7162c971d841ef04c2479c6b338a0b885760a72436ae4e30753306a13981L - Miller-Rabin test failed.
0xf4ff713c4f13689a6205daeec1fd3a4f2410dadeb60f5604ebd7247f9bb84969L - Miller-Rabin test failed.
0xfa2aab997b4940d4695089505737a7eec450652b958004017765b4b51506ba89L - Miller-Rabin test failed.
0x858c4588c17d319bda3ce25fa6e08a0cfe5c7280d03fa1726f9689dbf678fc61L - Miller-Rabin test failed.
0xb5185437df689e052bd16039ea7aae6df4baa0dc7e92ce2761492c96304e912dL - Miller-Rabin test failed.
0xbd383430a6b3ca3e765918f4d46410ea0b95dd37198ab68daa989eed10e155d3L - Miller-Rabin test failed.
0xe0db502e4d4ae8e8edc492ee22ac5050f7577ae2d40329d2500fa25907997a0fL - Miller-Rabin test failed.
0x8cc95f6358b8c4df7303aa211347895bfbaabfe377a0674838b839b689673447L - Miller-Rabin test failed.
0xfe24b3ccf42cb86b08e77b081768075e46b1312ca291fa75c10b43a111060097L - Miller-Rabin test failed.
0x97ca5185749e15ffa8c0833e436f5d6a06727d321cdc5ef6b9f595c4c4c8e139L - Miller-Rabin test failed.
0xbff83696f6006afcc899389eb0132e8cb23bb305e9895a5fcede2ba995c7df83L - Miller-Rabin test failed.
0xbce58cf36f02f58894fabde530b6d4e11256566fb6b68d196e3ef460d92c0a6dL - Miller-Rabin test failed.
0xb72c657359f88e86ede8dd0c261829a9a930af7a94e987fcd9991646d9ec76c5L - Miller-Rabin test failed.
0xa1bd3ed1c4eeda778ae66e01d33f1beea397efc9282375b1bfde6794d6f3376fL - Miller-Rabin test failed.
0xeb27b761acd83570ccbbb8252f18bfa0e4314e7a85df588a35cdb7f40c038799L - Miller-Rabin test failed.
0xfed4de5f39b2882686e8ba325857d7aadbdb0daa7fb3bb7c64ae8fe129ceeccdL - Miller-Rabin test failed.
0x93800e62f74fe727f576899779d8b5bfd9d9fe455de6963c956db965260bf97dL - Miller-Rabin test failed.
0xb390a655f8752f64cc095442278951d747da2bbaac11dbdc8f945fa9f4cbf6d7L - Miller-Rabin test failed.
0xf7a8c11b65074774a31315324fec17f260af6ebb9649d173de0a6b198351b785L - Miller-Rabin test failed.
0xb7bbeba9ab88adcab328c150cd1b2dba53b831194b33c5dc3bc11f28c8a439f5L - Miller-Rabin test failed.
0xd492a6d1b9ef3dfd00e5ce8070ea37bf609d6b0935f207945c03a9c50ae6ac13L - Miller-Rabin test failed.
0x9dc0edc171b9817bca1c9ad6e9a495153783bd9810af6d37c320af6d764b727bL - Miller-Rabin test failed.
0x97f3bf530ac8a82bf4ad05214a411896f1f06609121cb05d4cdcf5d617dfb13bL - Miller-Rabin test passed.

---P---

0x80faff5b75e995e3cffcae703f043a7fbcd5cc51b58af52e5a2be486d4aa7d33L

---Q---

0xa5c2708359596af0a67ca671642cc3c68cbf66ac786a43fec527b685df248d83L

---P1---

0x97f3bf530ac8a82bf4ad05214a411896f1f06609121cb05d4cdcf5d617dfb13bL

---Q1---

0xe66a7544cfb4a4ebbc9f7971bec574d7a999736d512a88b97fba6d758ef3f8b7L

2. Значення параметрів криптосистеми RSA для абонентів А і В

	A	B
Public key		
n	0x5383bd7b737be7edb383df63f876 0ecbb829f7a67ddc08059f3a707577f bfb8b59e16e5531fde82ff581f5f4054 3121a51e16ba248b8a7c8eae4eca8c2 5f2819L	0x88c42e6d128bd5247192d6efdf3c2 686e4fb204ab8981df3ad8a1d6ddd4a 22001f6a3234d9869e7a700a761364 9599ae2a8dad40c5193b5b4d21ffc6b 999d92dL
e	0x10001	0x10001
Private key		
d	0x12ae71806000e38ca48f673531ab 16fc33221027ca17a223bfce8ec1782 981c7145184e66e8768a16af53f32a1 8571b208792462712a2e5fe3558a6fe 2421291L	0x7c1c0b454f9f353c6d14239869abd c0a6da0b61d18867227bf43a6911c4f 39aa27db09ba7e75a63545827e272c ef12de5a99ce87c95d1a51af94198c5 5ed22dL
p	0x80faff5b75e995e3cffcae703f043a 7fbcd5cc51b58af52e5a2be486d4aa7 d33L	0x97f3bf530ac8a82bf4ad05214a411 896f1f06609121cb05d4cdcf5d617df b13bL
q	0xa5c2708359596af0a67ca671642cc 3c68cbf66ac786a43fec527b685df24 8d83L	0xe66a7544cfb4a4ebbc9f7971bec57 4d7a999736d512a88b97fba6d758ef3 f8b7L

3.Чисельні значення прикладів ВТ, ШТ, цифрового підпису для А і В

	А	В
ВТ	0x1729b408a68dafbc8bdae91c6c8b20bce3058660052225158fe07db3a031922cc405f904aa47a560fe430fbeb8c8b61ac1a53398b08f1cd7fc25ebb531307b56L	0x870aa0ed3c4bc777ccdfc730a113a8cd71158ecc4998d4d764eee901c6e775d636fe95e0d49ad57af3b4cdfd4686ecb93577d267183110b340bb97d6cc9293b3L
ШТ	0xd6c331f33f3f4572d845c3e7f4022d479f40c6ca39f8a2224db3323372e47df312709ef083d5306f9a6efaf8dbad63df3447809c97aaeb965adc21b4cf32e8dL	0x52c8d160696ca65b9d0c41b8e8677a3be83f460a5b88dc8bbb08f2d74396ca4ec14414ce3b70e33296c710898822bf6445bb1bd54826771b27802bc428cfd0fcL
цифровий підпис	0x2829fb7e4d605e7228ca16a9b92d316fad862617cdd5897042e4af328574e7a3672e8f0f83f3dbb4db2e5ada112571b11c843c0bf90d2ca1e515b7c29514f81eL	0x2728b30c2037416a56a4c1e68a921fafa7532c03a89dce4bc6a778c6a82ca6613e6b67a7b632ee7cea03b05315200fe0ea0a921a7f80aed477d5522335acee7fL

4.SendKey

Get server key

Key size

512

Get key

Modulus

A7F8397F572CD90F1151FC58E0939F5809B6E6D8FB7AC75A3A423CCF259ADC404F5308B8F965BFD1C5939

Public exponent

10001

1. Send Key приймає відкритий ключ отримувача відповідно зберігає його в e1 n1.

-e1 0x10001

-n1 0xa7f8397f572cd90f1151fc58e0939f5809b6e6d8fb7ac75a3a423ccf259adc404f5308b8f965bfd1c59391cbae
a90ccb9cf96a10071ced61f394154295dc93a7L

2. Приймає відкритий ключ відправника та зберігає його в e n.

-e 0x10001

-n 0x5383bd7b737be7edb383df63f8760ecbb829f7a67ddc08059f3a707577fbfb8b59e16e5531fde82ff581f5f40543
121a51e16ba248b8a7c8eae4eca8c25f2819L

3. Генерує число k інтервалу від 1 до n1-1 шифрує k функцією Encrypt(), що приймає на вхід та ключ отримувача , та зберігає в k1.

-k1 0x50557784547f718b581c096fb1df144f8da0818c861f348e0e6619674f025baaa1e0871911ba589eefb5d36f053
39bb63528d7511d5ac9c5802aeb55ea11d71L

4. Підписує за допомогою Sign() k з ключем відправника та зберігає до S

-S 0x41f5e44c7419dfe187d22465f726f2e6b00da9b51266b194ce7e91344ca678e6234454720513d9d6fd4c198fd1d
b0be2f1fd25d9fb9a8eb0c52c51b9ecd1eb61L

5. Шифрує S функцією Encrypt(), що приймає на вхід та ключ отримувача , та зберігає в S1.

-S1 0x4164af9bb37f9614a94d089cf8bf1f7596a670ec1c1590c4d3e8a9d6a2a26e969ef12701b8e3353afb1464f287
118384b37b739de11649be553034a268c2a9e3L

5. ReciveKey

Receive key

✖ Clear

Key

1a0818c861f348e0e6619674f025baaa1e0871911ba589eefb5d36f05339bb63528d7511d5ac9c5802aeb55ea11d71

Signature

4164af9bb37f9614a94d089cf8bf1f7596a670ec1c1590c4d3e8a9d6a2a26e969ef12701b8e3353afb1464f287118384

Modulus

1b829f7a67ddc08059f3a707577fbfb8b59e16e5531fde82ff581f5f40543121a51e16ba248b8a7c8eae4eca8c25f2819

Public exponent

10001

Receive

Key

106490609C4D1D7B45C0E04FA7B58EB90A7B6BF8C499C926F4D8684F90B89E4D6F24897354F0B0A27862B1

Verification

true

✔

Висновки:

Під час виконання лабораторної роботи ми практично ознайомились з системою захисту інформації на основі криптосхеми RSA; з використанням цієї системи організували засекречений зв'язок та електронний підпис, дослідили протокол розсилання ключів. Також ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. Виконання цього практикуму та ознайомлення з системою RSA було дуже корисним для нас, адже сьогодні її використовують для захисту програмного забезпечення та у схемах цифрового підпису і вона є однією з найефективніших систем криптографічного захисту даних.