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

ЛАБОРАТОРНА РОБОТА №4

З дисципліни «Криптографія»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-83
Тущенко Денис
Чудо Христина

Перевірив:
Чорний О. М.

Київ – 2020

Мета

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.

Завдання

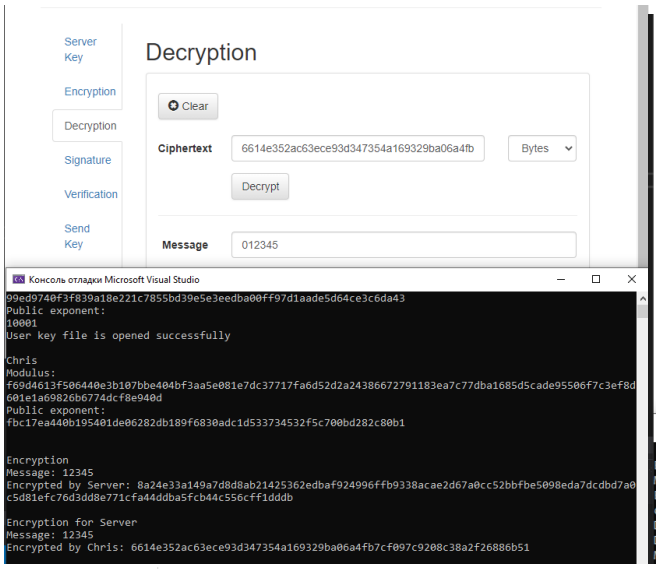
1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту 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 і довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб ; $pq \leq p_1 q_1$; p і q – прості числа для побудови ключів абонента A, і p_1, q_1– абонента B.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ та відкритий ключ . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі , та секретні
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання.
За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа .
Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().
Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем.

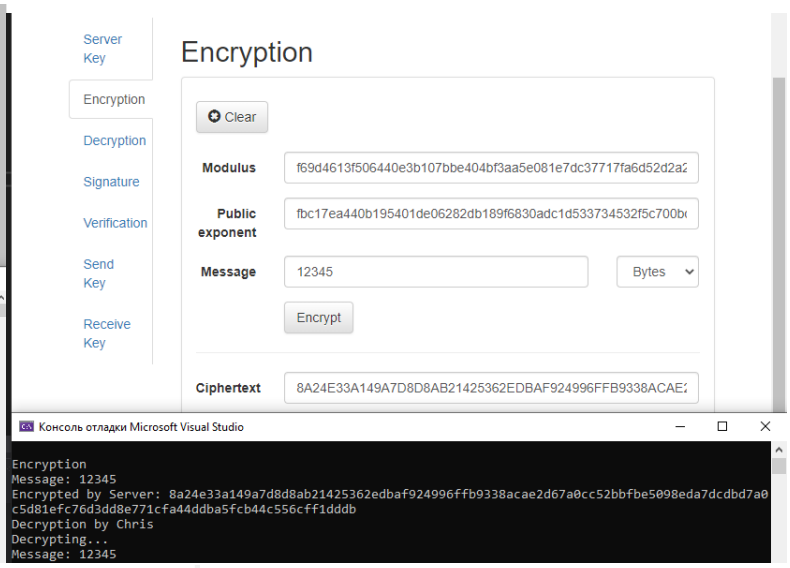
Хід роботи

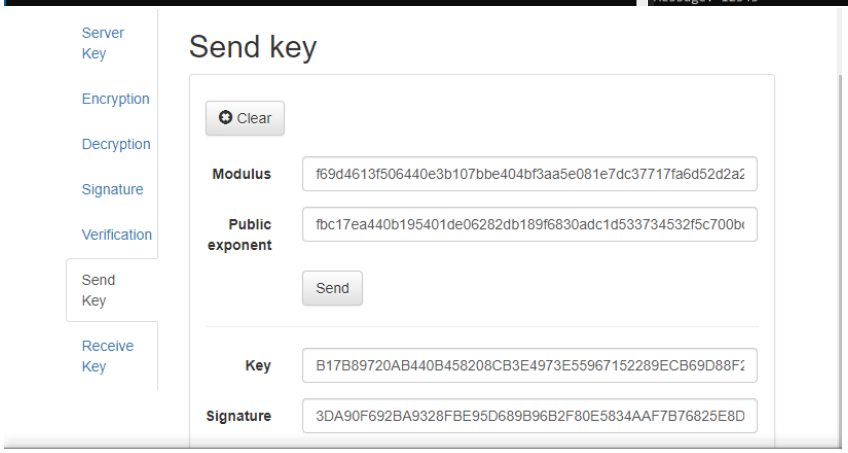
1. Пошук бібліотеки, що дозволяє роботу з числами довільної точності, та ознайомлення з документацією. Було обрано бібліотеки boost.
2. Реалізація функцій пошуку псевдовипадкових чисел, функції тесту перевірки на простоту Міллера-Рабіна із попередніми пробними діленнями.
3. Написання класу абонента та реалізація методів цього класу generatekeypair(), encrypt(), decrypt(), sign(), verify()
4. Реалізація роботи протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA.
5. Перевірка кожної операції шляхом взаємодії із тестовим середовищем.

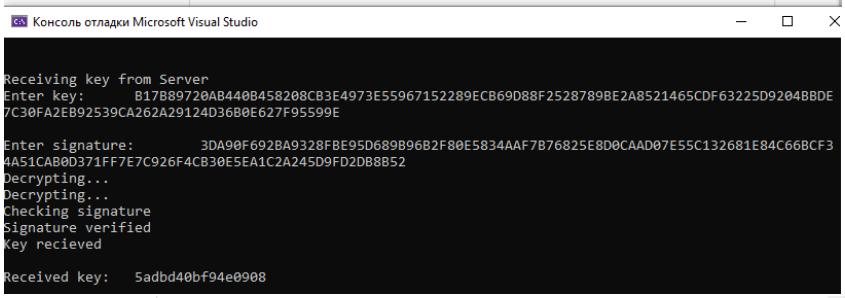
Опис труднощів:

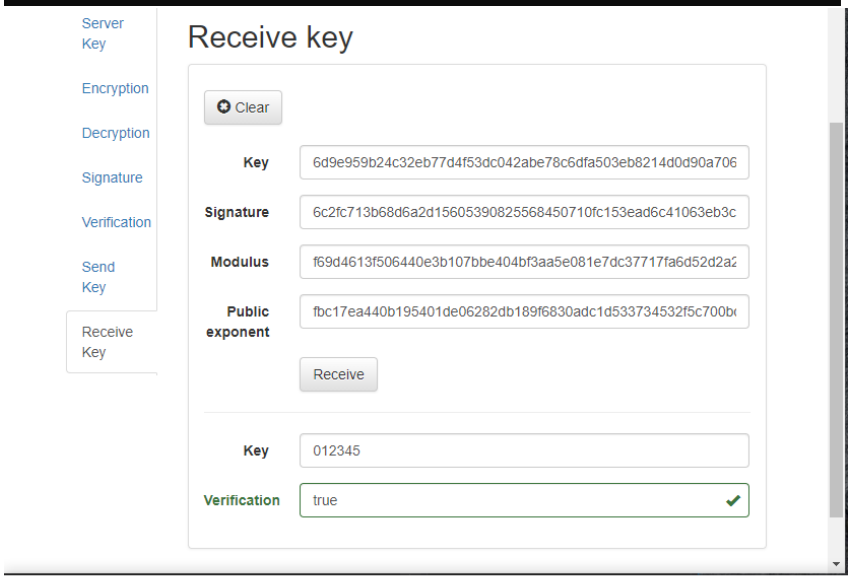
1. Функція перевірки на простоту за Міллером-Рабіном на перших порах працювала некоректно, тому p та q потенційно могли будти не псевдопростими, що заважало коректній роботі методів класу абонента.
2. Не одразу було обрано правильний тип даних для зберігання параметрів ключів.

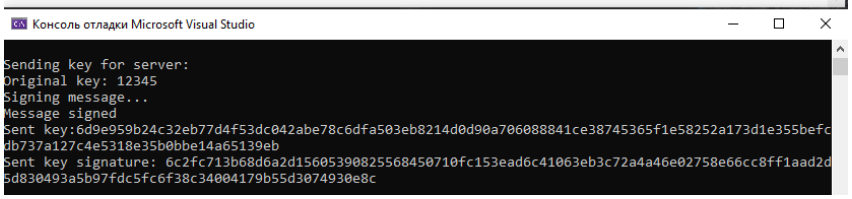

Server Key
Encryption
Decryption
Signature
Verification
Send Key
Decryption
Clear
Ciphertext
6614e352ac63ece93d347354a169329ba06a4fb
Bytes
Decrypt
Message
012345
Консоль отладки Microsoft Visual Studio
99ed9740f3f839a18e221c7855bd39e5e3eedba00ff97d1aade5d64ce3c6da43
Public exponent:
10001
User key file is opened successfully
Chris
Modulus:
f69d4613f506440e3b107bbe404bf3aa5e081e7dc37717fa6d52d2a2438667279118 3ea7c77dba1685d5cade95506f7c3ef8d601e1a69826b6774dcf8e940d
Public exponent:
fbc17ea440b195401de06282db189f6830adc1d533734532f5c700bd282c80b1
Encryption
Message: 12345
Encrypted by Server: 8a24e33a149a7d8d8ab21425362edbaf924996ffb9338acae2d67a0cc52bbfbe5098eda7dcdbd7a0c5d81efc76d3dd8e771cfa44ddba5fcb44c556cff1dddb
Encryption for Server
Message: 12345
Encrypted by Chris: 6614e352ac63ece93d347354a169329ba06a4fb7cf097c9208c38a2f26886b51


Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key
Encryption
Clear
Modulus
f69d4613f506440e3b107bbe404bf3aa5e081e7dc37717fa6d52d2a2
Public exponent
fbc17ea440b195401de06282db189f6830adc1d533734532f5c700b
Message
12345
Bytes
Encrypt
Ciphertext
8A24E33A149A7D8D8AB21425362EDBAF924996FFB9338ACAE
Консоль отладки Microsoft Visual Studio
Encryption
Message: 12345
Encrypted by Server: 8a24e33a149a7d8d8ab21425362edbaf924996ffb9338acae2d67a0cc52bbfbe5098eda7dcdbd7a0c5d81efc76d3dd8e771cfa44ddba5fcb44c556cff1dddb
Decryption by Chris
Decrypting...
Message: 12345


Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key
Send key
Clear
Modulus
f69d4613f506440e3b107bbe404bf3aa5e081e7dc37717fa6d52d2a2
Public exponent
fbc17ea440b195401de06282db189f6830adc1d533734532f5c700b
Send
Key
B17B89720AB440B458208CB3E4973E55967152289ECB69D88F
Signature
3DA90F692BA9328FBE95D689B96B2F80E5834AAF7B76825E8D


Консоль отладки Microsoft Visual Studio
Receiving key from Server
Enter key: B17B89720AB440B458208CB3E4973E55967152289ECB69D88F2528789BE2A8521465CDF63225D9204BBDE7C30FA2EB92539CA262A29124D36B0E627F95599E
Enter signature: 3DA90F692BA9328FBE95D689B96B2F80E5834AAF7B76825E8D0CAAD07E55C132681E84C66BCF34A51CAB0D371FF7E7C926F4CB30E5EA1C2A245D9FD2DB8B52
Decrypting...
Decrypting...
Checking signature
Signature verified
Key recieved
Received key: 5adbd40bf94e0908


Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key
Receive key
Clear
Key
6d9e959b24c32eb77d4f53dc042abe78c6dfa503eb8214d0d90a706
Signature
6c2fc713b68d6a2d1560539082556845071 0fc153ead6c41063eb3c
Modulus
f69d4613f506440e3b107bbe404bf3aa5e081e7dc37717fa6d52d2a2
Public exponent
fbc17ea440b195401de06282db189f6830adc1d533734532f5c700b
Receive
Key
012345
Verification
true


Консоль отладки Microsoft Visual Studio
Sending key for server:
Original key: 12345
Signing message...
Message signed
Sent key:6d9e959b24c32eb77d4f53dc042abe78c6dfa503eb8214d0d90a706088841ce38745365f1e58252a173d1e355befcdb737a127c4e5318e35b0bbe14a65139eb
Sent key signature: 6c2fc713b68d6a2d1560539082556845071 0fc153ead6c41063eb3c72a4a46e02758e66cc8ff1aad2d5d830493a5b97fdc5fc6f38c34004179b55d3074930e8c

Enter generator size: 256

Key pair generating...

1f54a9b57eed94c9ebf1ba4290645c7565b16c32ba764eee883cf9d9c1f93b62 failed trial division
83573f41f25328e30ab898b3f63ae74b9f81c4dc9410e36f074443d0a9649c5b failed trial division
b07df8f80c7d2d3f3288e571d2ac4b5a05879ae8c2f90f7964b77470f78728ce failed trial division
691087ce8c1537661dc54b90aad3af22d3ef1b766255b458eac0bb878cbd68c8 failed trial division
7e7882af3d784ca90bfc9364af28af16d50986d2a04c63530f6268ca693f7fd failed trial division
8b144cb7620a6427d702e0af0812fb1769d1e12ccb9eb15cbba3d8c5c6efe1b9 failed trial division
de97eb9d728d292e97937733650ad334f789ede17ab452243872ea6eb903e9aa failed trial division
cbf31fff71de1a8f64a871a340485c37928a11e5ab9b37c5b26a2d4269806c5 failed trial division
ccdbf0ad023cf82293a99f44bd12bee940c34bd50047bd4aa6ea85824635f8b0 failed trial division
e1f403eaee30fb6866e9961d53abc6cdf62098052d57bca9c81c2c1b0e022479 failed miller rabin
4c64a59d86d5a7e45d0cee58a7f706c405ee5650ae979fe9206c26d9f298b2a5 failed trial division
7fca5dda71671d763b33f48fab2ba8a6d376dbbfdc70e103787a56f8090d2eca failed trial division
ffd6eeacf3dd222bbc32d47179bac2f70de580a30440f46348d225ae64444b29 failed trial division
fee09d9f5e8d3e5c05b8efb54a77d37223b33c3534be48fcb4ead2dcfc142511 failed trial division
524462e7e767c49ee0ae0d981d08b44b726f3aef7e90400fb2a9a22c33937dba failed trial division
8c61d783802c09429e8b0db385db54c61c9d5e6ef6a0212e775f1e40efc2fe4d failed miller rabin
d2c8d606dac28d269246682e0f1d5bb2e13e617ba1b9478d388d9838955f6b85 failed trial division
8ef9d6e3aaa9e45c96ac0cdbe90fa8712062fd62f2985665757d3feec66a00a5 failed trial division
eeaa1929ca7060c3ba758e0de8b3e717f83de0255a4094de0853341ebea0da61 failed trial division
315355bb56a5a1d1b46c294c90baab6b94af609296ce44645342e258214becd7 failed trial division
e7eb78987064fd4cb26204bc81fca8dd80022a0b8f3a84186efd2e5edb196a1b failed trial division
5a9e127f0d764d1872db89e692611aa5d1bfaac03259128ef25d372c47a142ef failed trial division
b448e2d3b30c4e1c5e6943b720f6c08bde01b9a1ee77552661c5e21620ef1a7f failed trial division
6728e29a65c29398bfc75c598926ff90616e6567319317fdcc76bb5f2c37e3ca failed trial division
605d456ad7c4620a933afdaf5fa060fb3ba34d66dec0cbf4790497853d93b19 failed trial division
a47061395721eb4d3eba1806bb92d87f01b0399fc51613f31783dde3d53d6585 failed trial division
3c9585ca6097a4920ac66d467140d56e6c11f4a1f206351bcc9f3c635fa76bd8 failed trial division
cdb3830757ab6a1ec325d2690538e20e8ee85b8da36da208d4bf805079c0a249 failed miller rabin
d134c5c8bf4a09dc7ac0ecc2257d60b57801690569bfe1f06239df689eea351f failed trial division
8e22e0a9e4ea944ee52c9819f8dba2ef04fb3bad2dcf741b6c15f79dc80bbc26 failed trial division
ee09c14caaaa255b15648f7197598a81f697ac53fd0d0754b064ef711e421e2 failed trial division
924b762472d512dcd12a5f5dbea3c1ec1901d56db02116b680f0d95633b4500c failed trial division
cacc32f06cf91157dbab1f006acac33704bf523240871d9ad48163c217e5a6ed failed trial division
cc51a704b8b3cdd61f7765bb49cd1ac3a47c27f136a36f1b0ccbcbb7fe83060a failed trial division
aa7629e0a8710b23a4adefc6edf8e7936f5cfe74b1a142a13240fa85b6116a49 failed trial division
98e072731441cf3cdfa636a5f54cd15f5393d0c84e05d800b6e9c27d8d9d4ac1 failed trial division
ecd70deecfc4a8474e1d3d40b7cb97b8a95a20bcc7a880e54c61413e35984203 failed trial division
36d085ae8e06e969a411244e26823ee7a2dd8439a0fef02dcebad77201f5db6 failed trial division
99ee60dc68f711932311400da3dd18557067165b18bab672000cf55f578daf00 failed trial division
7943eff3f19d3eef59f4c796e91dcaf95a9e9b56e720d51fe73bac35f473edc3 failed trial division
839ec50a56385238a6822368e1c7cf6744eba7eaaa816ee1298ea4bf5b55f2f2 failed trial division
a3dd8ef0e03b6b21aeec2aba035974dc8b09043a650c562f209ad980d82cfa4e failed trial division
f23cf581e7aeb48fe3755159e9541a7b35afd31a5b122c8c0ea703dc99d2fb64 failed trial division
7347f5334d19fb0cd719dfcdfdd6752754f87092c6987876ecbcf58786cc56e9 failed trial division
1da4dcd205940f3040928cabfe16f80c17d1827bb6e011abbf5cc2339859c46a failed trial division
67624799e5233c4a58c47fe4ba5d57bf01587a6796526227d29dd754bc524150 failed trial division
88dc4772fbabc7a1975d983c5c9ddc1c944fecfaff77a886a37e828e72ef463d failed trial division
d5e826cd69c9cbee3c0c9537b533006a6a4aa9815c9d4becbb3d34f9b024aa1d failed trial division
195ac9dd58e28562e49f9e4a15eb694cd8135e16f70e16afd9dad7dad4f4babb failed trial division
a0f32d35aa03a5aafee106567d5492b1874112028852d691fbfbd022817d958 failed trial division
e43d345f4dc14e3d5eeff65d0bc1ab74f23995f205e4f78f8e27b261ff8038b5 failed trial division
f4c3be8e4962e12994a6f129c2978355a5546fbc75b2493a76d6140a549baa3f failed trial division
341890c0a658e82b15a046029e7ec95748aacd7e97ae4ca8df2f76fb4049b3fa failed trial division
90fe9e1f339444cd673099f55bbe244f2fe50980fb571af9fd47dce2926e0775 failed trial division
b1b32586aeee048a146c61a43edb62157da6eb9be19efe3f4938d6e9b0afc51e failed trial division
3f7c976afb6c153d2ca6cfb8dc744196ba4979da76cceaad3841fbbf2ea064d4 failed trial division
352e65f25ace7779f5c3a56a93b53656176f202ea7aa7fff60a3d4fd184b018e failed trial division
8e61a479bafc55c9920cc7dca46c591b9ddec843a10bceb50a8ff0133f282c95 failed miller rabin
987ef10c036dc5fd49305f6b39ccc0afd2b0932dcf4cd8fd08756c004bc4723b failed trial division
e6d84b72296462243a34564ff0533b11103f7b28f8318d8cc1a5ff5e7e050 failed trial division
343783eb1852691fb23c3fe6c4efc5cb35ec829e49136948bc41dcd9104333ad failed trial division
57e373b2a782e1213ab109d079d37b10169b1e040b8631231b00d3f1bf58fa44 failed trial division
40e54d9f45f36675503baf0c21331dd3bc957f77ecf5a6edc6693d55a1d5a9b failed trial division
673e287f1de27c89a30b7055d212d0da5d1f3f7072cf38e2f8be370fbac4132 failed trial division
2c0b85c21982e0b423b7b09cff615562d6e519300d8b21a6a640859b809f91e failed trial division
abf9d66aba161be81f92821e5419e5973134abe13dc93f5767be7baacaf63351 failed trial division
4d333c21ca7b3d7c3156145b13cd8564e540ecc79d17d71230bfbbc4c52b6b2 failed trial division
2382b1671c3f6babb106cebbb59e5aa59be429cf4cfc9ad550543cd246efb0e3 failed trial division
a187070cda3743d5cb03bb9489a80bbc1ce2badc9e1129628f896ce970b05c failed trial division
7b32d9ab7698ed309224bad85169cbe95bf345aac1873c87d2fb876816377ae5 failed miller rabin
62fb9cb37f0c6bee0464a3aa8ea5f435e8ba72dcca4f3ae44308f6eed93bd82 failed trial division
9d639cc9d755c3ce53b2041610cbfd34b11a957a4490dacb814d8f19e5a37a3 failed trial division
f81e2334e16f70c567b7529aa77a9066e85d55d74479af5ba05f569c9c7b4a8 failed trial division
e6701fbd3d3737affc640419265d8013536d028965da7c825c8e4dab1c9a0e2 failed trial division
b61e5e8bc565d6dfc3d10706faf68fe77150023663dbfa260aefad521eb4692 failed trial division
932ae309f573319270b30b505d969eb9ab7c47c6a32e2fc86504754deae0ed3 failed miller rabin
67c539bfd62cd1fad591cff75f93b5dc6f8f30447bdc0609786ac24e1fab9e failed trial division
1938a699e21e809ed749c0d20ce3c59f15bf0f6ab4f6ea60666d2990ec0ebb1 failed trial division
2c9b6771c13fa9f93ac2af181c587d9b563963d856a1a939668590644916b7c failed trial division
5bb2e537346746a7d43662025497c32c4d794f4f8fd5ed4d40c502e310808096 failed trial division
160463467eb76f5ddfafdf4862ae74ac742649cba17db6d28241cfc522dc07f4 failed trial division
1425775ea7e41236f036126533f47f0aef0ec886c5d5c4a6510444319bf2c3e failed trial division
73ea91460eb490b169b9ee86bdb545f1a078987b8fb9e924730f41f4fda849 failed trial division
fd5d2ec85f67fd246fda163c3f48b532cb0a6b547c27fd8cdf504cbb6afac91c failed trial division
7648fc4186e775d8d387c412173ffded283881e7d271b10118f78bacc1f78b10 failed trial division
8802a4c964cb77d18b18fd4968a0c2c25766a82e2fd6df6daa56c6ccd0186366 failed trial division
5039a7c3a4d9b3bed4928473b4422dda6bf903dca51de914807d09ac210c7454 failed trial division
e2d41993f5f298acc968e96ac7ce0cca46276b14b4becc9091c7ac3a37603dbe failed trial division
c825c0619d3620dc119330cc74a94ec187422ae75d6a3877af8e530c72392c8 failed trial division
5a039779754dbfa4e9289fc5a5d00865929c53ec983fa0d7efdf74c996b0a375 failed miller rabin
9ec34f673da38059096a10df22a30748babfeb2a909fe98c8af1a7725c89a10f failed trial division
51b438a7f590ab698c41a0a14128146092791 58e666b06d6cd74ede06e06f3ef failed trial division
10a7a1106460dd8defbca8ab4b6945c11832daca432fa975c53d60c63a562cdb failed miller rabin
839df2b5fd1cddac0c8dd257ab9ca173db274f648644555ba67ec20fac55a47 failed trial division
d87c1e563ace3e33ec1cd8fd370b3ae09285455e8b5237ec829b4c9a013f1f52 failed trial division
7097a0aefccd66b0dba0b393cb07fd1f6500cec75e9f312d04b544bef0d43391 failed trial division
7ca5f431cebeb5ad86f044cfe12d568c2b2312f82dc30f6ac8b428520bd6ba7 failed trial division
a552160ee6e7bf20a4f6d2bf2a84409cff73ee64e58bfe0761ed3b0111bc344 failed trial division
4548823cb9983351118ab809deb42c39d2e0088c9954e3e2338660e6c88f3fb failed miller rabin
e39fb73ebe8f2e709698e31286428b2728e65ebe6ac4d9a40287441d3cdc1c failed trial division
0c90b8c83dbf6c603e520bde5d6760e2ef862253c613434952a2bc776ce5b41 failed trial division
9a20e18f488996f5ede7d800d4f47ed48aa3c63803d97dc0a86e9f22c5937ad0 failed trial division
f8e3a69f4e3b61c348aa7809eef783b6f6d3ddb524bf58ad3cc7b81f6c9b535d failed trial division
77a833a213348786febde4c551f7f327da7c7bdbb3a606c62aba4e7f4b559951 failed trial division

559b4692cf47a338c06767c3d5ffdf239f55733fc88923959ed7b07f45e25628 failed trial division
88d7b4b9723873a6c8cfcb94f0d6b18c691ad72fca593f376115801799800e5c failed trial division
4c1070d6980e33600e3b7bfb05239535880b2bd3fe0e1b2fa10689d82dc8d6a3 failed trial division
e04e9358a64a25332c2a565d96030f1b7f89ca38594625c66c1852bf79b00078 failed trial division
84ad73332b895f55fff2672fdf9dcec4af552d26332c74db5887f2334c96ceb3 failed trial division
5d36f61f1645d19426c98aaabbc1c90e13ed21531bd6df29268c17194ba166db failed miller rabin
ffb79f784063193d92447367396f7267aa8106ca5ec330da293922624eaf213f failed miller rabin
4df5e7dc75a1f5e3c50b6ee880ad0d38ecd9f4b04d0ac412f17fce03ec8eefde failed trial division
94355104cdfec87a975f4a09587a449fa0d152ae9d79eae2c88f39ba636236ab failed miller rabin
6e4b78fb6f35e10812acf209cef50c24c51251f51c58cf28532d225cf81331a8 failed trial division
86c62e1b10a4e04deab57814a281c07bb0d2006902532e1c9a9204acb51e5fb5 failed trial division
2b5499fca59871ee73267dfae31a214be32f43335422326d5c6a198b68345799 failed trial division
80c61441e583fdba359b2572983a97478b4d7cea1f924af6de4dd333fb72de8e failed trial division
1400ec54e5c4a580725a8995e571b9b97f4a5c0395a4d1a88a0f05303f31f87e failed trial division
704a61a7fcf05083d14acd4ba65b6701ce84c085ced7c130e13a46cbb60a4b9c failed trial division
3d2e10dc1825e346d3534b429133c430a97235241eb4e76be44d556e3ebc7477 failed miller rabin
1c7aef88990b36d04697e0009b20c6de977321d4164486b1b794fcb25d2a4f41 failed trial division
7e174aae7e2568ab9deb0461afb217a6162cfa076cf0dcaa742d10c57b05c577 failed miller rabin
2b52eea72621bb80dd104cb78d4892f0153a6e89ef78d9464f5eea0aaf03e848 failed trial division
e1e5935f0a0d644ac2826e6e424435dc7814133646b4178a4c4ebaa6bd570837 failed miller rabin
a8bd3241320d98ecea4c83b9a31b2f1725915e6b5afa505d801ac866dd00d808 failed trial division
7eef30636b14e2b893e5eba522f0357419e9b9264b178ea8a47dcea0ca1fdd89 failed trial division
16e413d19c1ce37caca12faa0ae25f1cd759eb6bf90a66ae7439a4cf5b9dbcfe failed trial division
12fd9704d74e06a436118cacfe22b7b692bd62481b608392adc5a51f7da4a4ec failed trial division
2a95a66dd14872bef96f289c34a78baa10a2ad638b0889266cc3810431e24dc4 failed trial division
3aa7f3bdf61927c79dcadb06223ebb4f5f0f3985c2800e91d08568fd13544442 failed trial division
44e729b920065bdd033867ac5178edcc3a9f876e1f9b0647fe2583ef72c4a4e failed trial division
dc66b03628fecf671b12158e28bc2350339f5dbd9cc39d4890f86d4e23892349 failed trial division
d8db59552e0efe0d2fb983d5a3727bc0bf27726701a0deffac314352a7afacdd failed miller rabin
dc778f250fe9b3628b1f8e7b6f460a8b7a3deb64eec429476f718477931ba901 failed miller rabin
86947e77b453a42035647abdef8e668873ce58051cffc48a186c6667e8a06542 failed trial division
88279a040f512a8c4d4a584a76c5733245f92c5ec3b1f67700ae54758c1fab8b failed trial division
a5fbbda87b199148884b8caf9ccf9ddd8c3eb849474965889c72373fe25f0bba failed trial division
cc77eb9a056bda8acb16dfe8a09f6bcd0dfd58c44f25c2437939d3cf76d34689 failed trial division
a9c876fed1c57eab787e3ca9d5197c113422ef72872ed50c33ea171262defcfe failed trial division
4822f72a23b080ecc69f733622f62b3ff2d00c8161eafbf3ff5fb99f3bc3e951 failed trial division
39b2b30bc3043e1ecdb7dabc93f93ad9a4749af3fa57322013b9ce36c87636f2 failed trial division
90be6b88385dc8dfe1ea7ec67a85863c24c8d3fc8642dbe95215cfe7fa08d1de failed trial division
1f52b736d03af50022ea2386c5338e67614f9602573397a5baa6a73ff0ee073a failed trial division
4c416e0dec49dc5291f99017d3d836185fdd9ae83a90b5b61d7e4fdff300c004 failed trial division
96762c1c81e8a3bb19d5ef69cbcac17dc721be20dc8b3a4eebfd5be024811043 failed trial division
ca0cdee7459b16f5f7d8de29ef8a1f72dc3a0d88f267d185237348f31e21d529 failed trial division
b9bbf4ee12609658f971fbe7c5c6bcba259f9364a30183e1fd2d56ccf4ea6c2d failed trial division
63c88f6034af928b5583e068e03e13d4379c71e985800d305ceb04b09e87cdfd failed trial division
dd775052b93c5361cccee1adec3f6bfa1426b52e8741305d8e05a7a4e12b41b6 failed trial division
36d0e89374e713561ece076d0f2393eec5f97dd01adb1b63c7f48e12bc8d5d09 failed miller rabin
9001f093aa0d265a72fad22ee866dd3c1fbead55b910639089276e3e63471080 failed trial division
6c8828febb3d323ef20d87781f9012b75f7b9de9c4b3a28b9cfe092b0a44548a failed trial division
15e36599c01a71e58c44b9edd04363ba663b2b591c495e23f4ebaecf6209d23f failed trial division
70da261ec4794e75d4a0b427aa6df26e1c2438392e113d3c5c9630bb63ae6d6 failed trial division
826d0503630753d0d33dbf254566279d30b3a0dd22623de26d0f39034b82a01a failed trial division
1fc17bcdb50790f7fa82bb5c3dfdd53381c6d1f800b786bd54bdde7b77c1b20 failed trial division
efb0f623f3d62d165dad12c4e2d3feed2ee6ceb0f5dd5119bd2ac98ab09da33 failed trial division
7a428496a7b8ea5c962e603e21df466b90ca09183901bb87c986b2546876aea failed trial division
2c64129348a3dad427b9f3dd695fef31c300c31200839b64173a7920efab1cc failed trial division
88e6ba9af607415b8ec05561fa5e032d3a1352fcdb977565c33d3b8c46202f3 failed trial division
3c818735e5ba4fec5876e20f5fbccae9c7d6d5eab469abb7056eed282785bd76 failed trial division
27162bdf12abaabb297eecff70a31ab700ef26e082546f240389d272f27d8944 failed trial division
4820e9fdb2b194e41ded8b00e1106d7603ebba77a8070f4e91c5a03c9ce711d5 failed miller rabin
488e8849e790852c1fd578aeddceaff5991dc5f70a37c7fa247e4e78fcf0be3d failed trial division
7492d4da792fdd5f7e6aa57fc77a5a56658e180215966d08eb6cd08d69f22054 failed trial division
0ae7cc5483d2f84a908e5de755dbb54d23c3662902161f9ea3bac699976bf7a failed trial division
d887bc7905cf1da3cac0ff09bce597f61d02577bed6f6dc34e6aaae225e9d1ba failed trial division
688611708bc6e5d57e53a832e2d56e6ba153865c8dfe7e04e7d926b9e44da49 failed trial division
b984e649bc79a0175fba7686b050ecfb3609181a044bf96125b8a9bc26a150f3 failed trial division
6f3a4e0c6cf11f56a1ae6ede7903605c40fa0465fd7abdeb94b6ef19266f4117 failed trial division
3293ea99a4e17c69651ecc0fa5b7f0acc8c8acfb05c8af30234163a200685d9f failed trial division
88f6c9bdd14e3530d4195e014d21888ed79b0ea22a31df7b10ac513060cd2306 failed trial division
23dbe0977ba481ab75612fd7ee7973eb8241774b58c268ee373c22e5a365589c failed trial division
189007d8e399e472e90761ca6be7939f74a14c18d3f8cc169a6ec1178d6fcf75 failed miller rabin
55ce0aee23d7d7bb4e532eac9cc789328f3ea4e2f0638113c8637d7dd5bbd4cc failed trial division
ab6ad014a1fbaf382d29ed3141c651d70a3db62d4a15013fa853707ad8e0767c failed trial division
d73bd698bc717959bcdb0726b1c70236e4fef94134cae07f2965aeec88c7d60a failed trial division
4aedc158583b67ee1306ec44cab8c1d4c19f298f4cb99d153798a86bbf2570f4 failed trial division
2d86a05d6ab962c19f64c2dcb87e1502e22c6714ea44e83296361b24d8570c6b failed trial division
fdfaa8adc427895f02ffe9ecc0077e9f90af57bb35170fe96c065e68e4b76587 failed trial division
efc111885a6b4451a3a3f9f39d578e77b3e6a7613a0b665fbbc7f155a3ef573 failed trial division
d6a9c95badd01e1209984cd57365779e1974171154de35ad9d2f345f920d8448 failed trial division
9ce66eea12147454ef7d603db6caeb5ee5f0efb644e7fede75251d1c043a1b4 failed trial division
c043dfbd67531520a55d022a09912fdca220d52c7f9155342caf291ca30a1c0c failed trial division
dcfb6750cdf6ea622f06456ef2afab14438e426106ba9f09f369273cbdaa0583 failed trial division
32e63149bbbb1030714336edf8bfbe599d7fc729d3771cb80d90a7757ed1cd02 failed trial division
4a2b5516f1e6bc8e9750eb9282b6feada732e80e2a5824d49a664a7fc07e20e3 failed trial division
4c85c7b488bbe41c61a3a084da98b45ddf69f3ebd3950d5cfbe87a75c17d651e failed trial division
845b14b83f1510d0f0a72b79125bcff1f0d4a9361a5c61a7a7c04a4d510c318c failed trial division
2aeb79db3f14848ac5cbeaa0e39241c20a11294409e546ad4d52e46ddab49296 failed trial division
6d2400f46c4c40ac221359bcf3bacae8827771f15e2e5d09f595d7da70787b2c failed trial division
2ad1b643eea4cd5cab1dde4d14349bbe3fb21021e2524a533d25680450d20249 failed trial division
97dc8e8b184d19084276f159f6bb5b864c0028c0e86d02e02e982dfe848dfa2b failed miller rabin
365782c9bd032248491dfad66179e581a20411bf83d52621e6bb304e348c87d0 failed trial division
cbe9440965df86640b779ce365d0bb05e6e5492a57126d3623acd67c0b798a44 failed trial division
fcfae05865c520bee3865a344245e9653490a0fa71bfe334c716a5dc25705df9 failed miller rabin
6865f7e5c58ce8bf89b5c445fd2d5ca5b976d84846ed11eae94ac2da7e7ee2a6 failed trial division
4cc5f706c133997ae88820cd8683c650d8a8956c4e85a5c4a89ab9bd5e432f6 failed trial division
2b02a098b14857ba604c51298b79d622dd6108de086bd1d51a954c770f1ab68 failed trial division
275ca0391af8c0dc2f41f12f4639215fee681bb88fa2a4ff31713f5ff6ec229 failed trial division
94df5e45ce9f3ac0f77c817dc21d7cf04981fe762b3eac993c8751e035b1d385 failed trial division
32f12920a29fa3793029a36d8eb1182cc56976916e31af94d3690ffe92ffba4a failed trial division
8c41d34fce1a30cd2be123c3f420227320b69f549fb97746e2fe1ea417c6dfb7 failed trial division
f6931e27f8cf725bc2747d61709d0893e72bf7e869d68616fe8a43c30ed77ed6 failed trial division
83a680dfa1b599fc2c32cae0f08b7764b1bb7da5e1f1d2479e44669c53b99b6d failed trial division
02a43646c82ef7fc6dafa871a2b41d4bbc30a3a111056a070cde0fc36aec2f39 failed trial division

23bfd7c0d59943ca3a45ca80d74b0a3ac5fd4655b6678441ff60b15d141a2ad6 failed trial division

7c2e241cd02f3703923b9107b0abcf206ea5571c792ca88f41f8d94556dcf9bd failed trial division

a178c8681f14755db51d3a0d34388703c3adb86bd475cf0c8ef05e94327fc618 failed trial division

ef99fb5f29f0b8673768adc0542033cff93c495f3fb40441c22fede592c03497 failed trial division

7835187c368f3042a13210beab7b9badb2bba8bd0e1f3ee1d1d6b65dbdd6a7f8 failed trial division

cfa1e9ebc4a316152a69f118bd0b7f0fb9f57b00bc9ba5260b78c0ccc796eb82 failed trial division

fd1a866a2b630bc14652b2636d5e69918014443fccc8fb19db50860d1a18e037 failed miller rabin

15bbefb358b05cfd17a74ceff0eb803ac005bb219f4050f865ff25ffbfadda19 failed trial division

5b84759483a292d5f6f8541f8656b59a5aa8e186e47e108dde8e6d5fea11aef failed trial division

27663be4d29621e8ba21b24449227ff366fd8e40049181154d39aa2aede62e95 failed trial division

8e45adfa52404fa152d39ec8335b0fd5d2f5c8b7f6ae1c6e6f2e71093410a8b2 failed trial division

b07b99d0c903a46b0534f4312432aeb34ac1be25940e4d103dbb88569557d3d5 failed miller rabin

34b3a079d443d6fef729b76c0d5d6605c25aeaff829021700312c87c207ee366 failed trial division

5a8fb229961160ab4f262c003294deccfbc9bd2e31dbac5371ea7ff513e46f39 failed trial division

82d1147a43ec277c8097b0b74f298c40707e3a4213f6cad065349f5f40395bc failed trial division

994f787039bc5166d196a112de47cda5e2f622df743a74231543969467a74cc9 failed trial division

bc89047697fe98d2330cbe7d776c8b3ab223a6be11e179ab288f0cec86906e16 failed trial division

fdca78529b958a19e7756fc4421173557a8bbc227c70a4b8d90633f36f54ec98 failed trial division

c1d105039231246cc2df7d123409ede1aa9b4854e63bef8513392546d9f6c87 failed trial division

3716b9f7fb50Caa6b29262504aee73b811a26639491cfa8e2337e9e547f7a6b3 is pseudo prime

58a927dfa191d91a780fd38070a8ff34a7de7e359f615b671fffd790251b15e8 failed trial division

5ff9ccb1e1fba57abdb57ea3132b9acf58b44be8994da3b63e1b55ba33a1b80c failed trial division

3f456c3d507dd1294386b974f7c1d8d10588cb7ebf39e420df46d3c279b0a8d3 failed trial division

149db8027d1d4d2ecf4c910bab0dc725633f12f55dcf85bedf3128ebce871645 failed trial division

d65d5e9e62e3d32a3c57b1346bc48bf534b90d6233713dc53301e906cbf20b6f failed trial division

351be52bfc1c1639f7ad19d6b9079a78726ae73cd16837a4f7a3e23f82fe4284 failed trial division

216a4764e86476f629125579720306 72f13db0251b57955ea3a22d6565c4c37d failed trial division

f27752e16f0a2b755c61322f5f0ab852f9740b32bff5915f3b5c0343ab7e72c0 failed trial division

a9df9e44d6cc3a41a053cc00ebf9e315b87b26a1be851091fd016d1fa9310215 failed trial division

b8c00caf7dcbfb3daba97adb25c98767172b89ee8007ca55d52766ab4e7cc8ed failed trial division

26934adee500cf4ff7fad58399826ecf0e6563f287809c3bd184a1dd408a335c failed trial division

7cddaf20998fea568c82e34a6ee18216d0cdadfbbf2796fb2e5819249e53911e failed trial division

1d7da2fa18333e5b1b151858bd59326840d406f1276a75c468d530c7083f164c failed trial division

6c830f64d073995af42e6a148f67470bca2c8507113fd5f1c01dc969eee811b6 failed trial division

1f7b40e9f7f47c955006f5b89c81f62f0c346d32a81f0e99cb10498ca21c55c2 failed trial division

299c746f04509f4ae6215df81bde6b5463a67023b716f763fa931844222c97df failed trial division

3717031d690038787807d768cbf48012ec5f2e5502c00d89536df2eeaccb0b6a failed trial division

3634bb0d0b1aa67b01c57bfa65f43bf15eae7bd77622821d4f84b63ae5fcccf3 failed miller rabin

e8c42ae7648598a37125e4e0b5f9d677008c32622ec1daaeefccb1e2288724b2 failed trial division

978d187d095ed41abcfade87689de6bcc4936a7a9bd3677568236 18003384fda failed trial division

73437685148cc3fd5915877affdb798b76f08618015585be347753e5afa5808 failed trial division

2474cfec7dec55f903dc3adc43be21465830d66b3d18e9a718a2bc123ad724cd failed trial division

a6540c102c0aee998e1738fa16545e5b66b757ecc6b41899edee4efadcb6bbc3 failed trial division

7c878ba91253e5c334fc9839ae045e7838f3c45d5836ae50fe8d97f0d318bdb4 failed trial division

27cd196849b31cab3b3e45b613b55978365ca946e4d3412dc91dd6b928b04d0a failed trial division

31c56f9d14e8a98dabf54a7da78d59bb19bd9f8279234b72f11380e5bcc749b7 failed trial division

7be8bd1724cee204ac70eee2dec5f81daee38edb73857abe7346717fdf8c76c1 failed trial division

f57f8adfa72dccdb68b96ab03de12b9b2a4f65a848a7fb8a46fff5fef194043 failed miller rabin

18757071dba150f1b9b1301241c0402b1e9c7d11612c5b72e81c3cc2d54f2f17 failed trial division

df13613b66e2914401626d928987199cfec25fb0eefb6ff5ad30a1b29499d0e7 failed trial division

a7571a5295afe87f1983faeea5c5809a832be367aebb33f3999a6da11ea0ecb2 failed trial division

87116415bd5655f4387836aa838968408179d8b5514da331eb1d62fa5472fd5f failed trial division

84dc2ae273caae9e5248b824a98e62d63bb77015b6cd90d55ff684215002d786 failed trial division

abf9922870f255220d8341059cef37da9766e0407bc001a48692abb0d21dc3fe failed trial division

8526c50bb2de5797146818d1770a594cef9ffc1038efe26d4a67d2116c5b970 failed trial division

efdea962ee46323b735f23bfd7451b7a841c52cf97f42e9c928ad24f6af0b2 failed trial division

22670b5748e206ae640a5c0b47b85c56be6a8d7a85a9f41a16740b8dbb4fbe59 failed trial division

3baed8e8267017db2a4cded5ee24f9cc2d1d158bd16e15ec02863ab1580cac73 failed trial division

456a902ea0b6b23a1b4b0ee0ddf51ef47ac45bf66226756a60eee0ebd5dda6a1 failed miller rabin

df25c735d225be5d0c223f23c0bc1c6893e85ff9c41d5b8b3315e9c5fe972f20 failed trial division

0991f47d8cc98d44a15b03c0c01aa76416e0d720d9bcd28ef65271705e435ed failed trial division

c784cf2fe6f7bfc87550fd222841521e97a225b87d1274121fff941bee822f3a failed trial division

b343351688140cd3daa27842925d6c3ce3aaeb753f6d6f537184b1d1b76dcaff failed miller rabin

1dedee1b03359ac35090bcb6cca5f8af30f32a25d77e1585b5ed5ab6876eb5d8 failed trial division

bfd726c9eb3b9b847c70cde30356410361b89aec7829b9645c2b409c85b76c7a failed trial division

4fb85f4177e89dc514be7a95a74a6f7e32c974ed01f530d082683966f94d1424 failed trial division

c59e1276b733232df52ca2945bae574615b58f2150a921f949eec11c1a27190 failed trial division

5e0e38a22b9351ce49d60bc96b56f1778210b49b7f7d4cd0bc76b63cc9ac31e4 failed trial division

18f2c4371f6629854e8ffcfb02d7c2cda2c32844f790153820b753398e243483 failed trial division

1086876dcb7fcd1fca88579d93939a5c94501481f914b67cb89c22f02504a3e9 failed trial division

2e188b324be57832bcfc0bbfcb8b0af2ed09bea9f242effc4ce54d3e479df693 failed trial division

210fad797fe797fec12de1995065882361045 0ac6ae421ba0eaf6d21bfefa57f failed trial division

a0d9a4dfc6e0b8aa3359908a4bc6f53b2ed90523930ac7b1fd87f682b65c2842 failed trial division

89494837b7f6897f57d402f6314a517cef3413ad5b61b63c276e11408140a95 failed trial division

15780ca9b3c449cc9abf76f6abb161727badf603f5ac8442b322d37e5c1b50e failed trial division

d3cf649b7ca175d1fe9479445a458075626d0958fcef5a791dbb36494ca9bf3 failed trial division

46d6f8d22133ca25713a254eabc8c51caeb2c7eb802b31125e306a2e1f7cb14e failed trial division

761d9f4e6d0b19611b0fb54a1753283c03d9468ed3aba7a849a1610d2461909b failed trial division

87298a35947f999d8e4eb0e5bcb3abb675306b0f40cb588539508770356bf0cb failed trial division

82ab4d7f2e6b6b24cc3db80215b49e269bbfcdc2de501b0b15c916d090b11fb failed trial division

4c37cb599f44c71cf9cb2614903622ea88fc6f22a5e0b89912c0a910579224df failed trial division

790858737d3976f2b70dd38615d6ed2278bee4bda1a109e497d9c2398a9e65cf failed trial division

278122268ffa0e826b040183912102d6fda294c3bc6fcadf190f8cef71cf4499 failed trial division

21a3ff136cc350598ac40fcdc1429e8a2712057c49ee5e83a6c0fa12a4dba263 failed trial division

f11c175fce06c3f3ca3697abded531cd41762e87567f52d25c6382061282044 failed trial division

20d19a3951aa1e5745d51aecd21c3b557748572cc52ba94300055027b2f95179 failed trial division

8fb07da11a19d8849a8165b5626e629ca1ed2a0f025f0d4ef8b24121e5cf7d9 failed miller rabin

6d465baeba7ddbf7afe2c951eae3b3bf5a9febe94bebbab2cd59caf0a6d1277c failed trial division

c39b9df7bd5844080096a9a458bf9ac94e2e83ba16f3148ec44e49ad04503543 failed trial division

1e815389f5aa10dfece6a8accd4cb9195fdab93f4527c1a9f19d09575b1907c failed trial division

24cd00b953e1a3e1d55e5f6861f5a08c584582288a561814cedc6c709e0a420b failed trial division

719f549377148ba13157dc27234077e0c4ea21f57cc937c3906fb118b50e367f failed trial division

f2bc836c66da15b37150d392b1e7384a8282bcf5dfad9b9316d1572eaeb8964b failed trial division

e640ac02222a623e78640061a65690c5babcb5de1e4c2b9981c473bcd8533f9e failed trial division

05c2cc8dabaf3b68d8c8cd9e6f0bc76f0ab29fb7cdb73dd5c00ca99af93770d failed trial division

ea11af5dda56a8bdc64ae4634967a692cb9b905aac0932161428cb782be9789 failed trial division

d817781c70d0fbb3be196819848f98a5786e74e4043937c79f69e7eaeeb1aa2 failed trial division

584dd74449a3fe899585035ff452e43ab41bcd7bfaa5d40879c41fee7277154 failed trial division

9d94785f47b925feeb35feac5d6e737bbc2edb736dbca5df5bde9710936e0629 failed miller rabin

2e318bb2e675ca57c7b28d490f850ee110ef60b990f9a89d7c3db3da0e2014c0 failed trial division

865e25e2107d72f51c8dbc5eed9dc03a1fe90836660d5dd58eec5bec78bb260f failed miller rabin

5e43cdd2838925f5b2c8ea3dc9fed91be2e17fcb8c5fb54797aaf3c79af12e1f failed trial division

de6d0d322f9327c64e8a493eac72ba81891da54a44c5fef70febe8c88df8ce1f failed miller rabin 61404a29b400fcc37ce50cbb2a8e0ecb636543bb0d88a7013cb545b86fca6763 failed trial division

290a79031cb8dd44abd5d18136ac651ad21a90394c685ba753b544bfbbf99bf failed trial division f2f0180cc852dc2b8526b2447de471588c65b6f1e346a2c2212b1baceb79861 failed trial division

bfafe4a575cc1eebe687768b49315098e67914f1e663b9e4507033a8b88367de failed trial division 7826cc59700f3c08409785d65076c0dda69146b7b44d614d79b4046a84c14a33 failed trial division

982d1a9b54786e2555bac7f892f10012001392ed8d9fe67fac575cee4337156f failed miller rabin 57e8feb8c780e697f3d1bede804a8ddfbcd65e65700c8c656bb24258195d5ec5 failed trial division

9636dbcd3345347c39bba4cac9afa2b3efe9d558c23a62d1c0412c8969007046 failed trial division 8b923fba609f3d324dfadb03dbecc5a8449671f944785f8550a1f718b38dcd4f failed trial division

cceaae46ead12ab8ed694bd9db1058e09d205533189ab9be2226419bc3f9814f failed miller rabin 1f70bcd603921007c478c130b364e399a9e4223288a557875349d66d1b35a162 failed trial division

ec3d77ed3a05c3386d4ec9a745e5443659e2fc7729a6073b2e079d511103c09a failed trial division 24686703b6b7166c32673366951b6152235dab3c6c660ca1f6dd0e2e377fbf56 failed trial division

a495a2e28f9963671809ff5b25a0c52d64e18760d3ca528fa60e29b85a036d05 failed miller rabin 42c73336abd25459f95cedba4eb79b247152064d9f746b856f345c737b3d3ebf failed trial division

f93faa1651c6b285756e4fb0dca40652f6f6d20801f6b5adb4a918febae8f992 failed trial division faa99ea49727b39929d1c69a0ac1224a3d37923169dd1bc40a5d39a77354e036 failed trial division

f3f73e19fd0091ef22cbbb618470bbf75399eefa0d0273c943fcc21db68e716c failed trial division 37223495c4a76e6292a9053ccd4eacbd3528ff77c4bc759a7d0b9ca0110080ef failed trial division

8b6543c3420edf041fd0ce513cd5073e7c516f6deecbe899e0c2d5c36280d590 failed trial division 28c359e6430cf48d36c9a3f43e5b30793c182b38070fd1484e129cec6b0a86ee failed trial division

fed6da56ff1ab5ba93f8645d173d107d37ca52518d8766b96f7967fce297054c failed trial division ca6270e3c0ba68a9f8226ddb1ffa9e2fb4fe958a765ea0eb1bb0c0b05d55912 failed trial division

e430d01c2126e717c901424b8fd31296268168d91d75364e467681066e55e1ab failed trial division f48dbc26bc596b5106577381ec6e41e58b281eabb320a6a2899a46a0c9614642 failed trial division

3aaab8311993aa6ebd7467de362d013fcd71fb31f1749dded061d904217722b failed trial division 5dca395d0bf50f32663db48d0bc953e4be39e4943476eda922b74ce81a6b360b failed trial division

b09802c8f400a76fc637718989881be425a0cc1ff743b6ad02baebc04cc517a5 failed trial division 879929c6719356bc517935d72ac506c848dbacfd8bf50965740bf7c603dba2aa failed trial division

ebb12f4aaf8e2c280f45a100a4efa0933db8abf3f526ddcf721c69bf5153ebb1 failed trial division c1ca3cb4c7651da35a671f3391db20214db350d9075545501d0860c7d79eb9b failed trial division

40bce580fbf46139df4b8affa5385de19950b1f444f9c637f4fcc8e982fd4010 failed trial division 464785d21ff247bb568ee80476029efd64f2c5c6a0d8dc0cce7cbd5c7cb671c4 failed trial division

79b359d6ec00bf0a6381dcac8b72995326e06bd0cfb476d20c22f6805667b14b failed trial division 23fe9f12fb742cd381a6430550f61ab66e77f8a739ad0eb07cea0ad09218a77 failed trial division

796f3594073a2ebb3b81d0419bd0a13c45a4ba0e1e76000e10ed5464ff28d636 failed trial division f5381fb1bea393a6487fef8ebee23c3e0c15fe0cd761d12366123463d270b6d failed trial division

987bcb45cc0d1c76d3dfa9d7fd21ad92f0567d31e3ea4d1b7ca9e965f404242 failed trial division 76c84f1047e0984d24a84103cad64de4bd528ffda2c99f846bca2283aa7d67d6 failed trial division

4da351c2605097e7a3e739cb79bd90e75db65fcc82e46d5142e5d399f0495730 failed trial division f0c166acb745d2320fc4f74c5a6d2506e8d0992fc5acbb884e364008fe8c14c7 failed miller rabin

7434beaa60e6949a38b740db227011509f66e216e71ba9c0510713e1a223d723 failed trial division c6708c104928e9b07bdc848c4be01874022329cc95118b1dd4f9a9e7523e4413 failed trial division

c2895b3f75f6f2a73d417dad4715216f6cfea6a239534b439adbafe1de8ab427 failed miller rabin 99a64b56562a79cad1a59e4656923adb8e1255ccef95914a7957de4c68786279 failed trial division

d8fbc8a5c9c16cc49d21fb6f0a4e6b5906ed96e152e4d3042dc92684164e7eb2 failed trial division ca40bc9c5f5cca81b0455b949825a75538b05f8424247a64d0dfea42917ae75 failed trial division

8f17920b59f4bac25075dc559eea9a727039db31e815e666dab546bcb32be6e0 failed trial division 6a0d5289c5debdbc9b0a62bdbed09ac1ad6d1039a649b91232c3562bfb762a8 failed trial division

122c4c2f42e773de26ce06b958b139109ce632d92a0ff7b4ff8074690fd8c3c4 failed trial division 7cc15582e96508f99e1fb3dd7c9767cd867d9ea8165e15239b9cb433101d7b1 failed trial division

b8e3c000c835a614e647c2b3561d6d54536d34ada0d90db242fe6d2146f07234 failed trial division e3688aa865be63ede733d5bd29e1b2aed58b7cdeb90719fa7012e803c27861d failed trial division

8ca55d2f543a8a486ef0ffc59d700fe4e3b1f6b5b1dc4e138edbfc9c08deb8f4 failed trial division 284cf3f6cc0bc69b8857bdf78b16ab909e60f825d3a9defc12a3290bd6c310b0 failed trial division

dbead1094fe47bf7db639fef70678acca301cf2d0bd85082ebec5c2c046114f0 failed trial division fef39e3a2bf02f5312e68c19a6f719705439cd80affa264fb34860ae007a5265 failed miller rabin

ed04c4be03fedba273320ab25edd5a710f4a59dd472445475c770dfcc12d7259 failed trial division a11dd04f0827e47ceb30d1ada8cf0a64ab9fddd4d6fc08068615d3bedaf6b7f failed miller rabin

7e545404f3575085af11c5818b0708f16f35da2539314120095706b0374cb636 failed trial division fcdc01f77b2030433f0de40b76ff1c0d56a261cbc9e69988d1afffb1e55ea1f failed trial division

ae73d047ddcf7937dbffbb5d13642aa00063bc5c1197947f8e6edf0cf576522 failed trial division 9156a69dd61ebab4d28b867538bb79828559e6deeb079cfaad4e9fd846329f93 failed trial division

bf9a9bcc7f8b08dc16a1fdcb0d8913260c498af4fad248f755833d9d55ea222d failed trial division f59085bca2035014121cd2ab715d8e1389582abedc73e3d95fc2d2e7796d2ab5 failed trial division

24737cf03731b8a22822b05fc09932b3d03e9f29de2e328016424060a374c955 failed miller rabin 690722eed9b6d0d1c28a6d916e83719caea6d04e66e82c2a2b9e8d570209abe4 failed trial division

e97a3e388551a4a06b2a9d8360e3311b7c399894af3d44e7f9f64403d21ccb94 failed trial division a4fa63a8346c264a3a268bf774fb736d096ad99b97bb72e414743c417b2fdfe1 failed trial division

6a54f5ec943f9acd69b73e19eb6db0fcc4bcf7dcd875432c89e8c5c5a81f6808 failed trial division f9faf160d68ad4df4ce5a401c07b4018c4585e9c3ffaaed399c37541dfba09c4 failed trial division

b98afb4e96bac50c625a091844a9ea056c013178817eb270ac2e8dba0632efe8 failed trial division 467bf17e6e345f68478a1358659d1cc110337de0c8ccd931d186432a01b3baa failed trial division

bb54cd74518fb0b0ddd438d8fbf833628aad00df1f45d0b770c63888e724a97e failed trial division 76f98f613f616c1612d73c83024a17faa19fc81c464dee2f1fd4f7fe1f31b7e failed trial division

199943b7ecf29c3037bc3363727b7784a4d01e5ae7872092c34f8352630dc420 failed trial division 3b8a2f7a20df3dd1c5112e88aa89634da00f21e375e66580540d0a5ce597aee3 failed trial division

1ec548cf9cde55142f81dbb7be3a1c240c1efe0942e391fdf55ef5d4c82e004b failed trial division d10d0c9fe1f6a92f1afebbe956fd422b55cec322da456397bb3ef84898084b8 failed trial division

795a80ee85e551231b733b275c13a6645f618afe264206a9a307caf8b047d865 failed miller rabin b94c4b5ae0bf4810c24f3a6031e166dabb12a580d00a76013a41d089a3373d31 failed trial division

c488dd991d9cfb960e6b27414206a2cd586585519931cd305f1de929785e5893 failed miller rabin 63dfbe9b72d2ebbb7c1c8e5edbb7b920e19ebf6b5c838ea5ebc6b90e053b35a3 failed trial division

33c662460c7f37e5e175af0b6b20efaf74a09bc6d402e633fef302fc308ec40a failed trial division 87c2bf9752b359fc234b8860f9b905bb518569a620266dbcab39acaf104499af failed trial division

cc68840559955b2b9920026e8d019705071852158cf5d0f28ef3e30dab366abc failed trial division fac2a5ae18356080c573284facdefb7c781ada11ef83e20b74dc8496ef0c203d failed trial division

bf1238f594ec03ec8cb26c0d964df1bea03762077b0ae469833f0f5309a190d8 failed trial division 8cb5fe25361ce222857f59cc32e397feb8065a42e690ab27d2e58c6f06791e2 failed trial division

565f81a1c9483f1046daee3686addbc57798b5ca3a9d373fdbaf5493b9d50fd9 failed trial division 207b775bcb6f4daf10b546b3970a0daedaa55a112ea14fd865629315fc176702 failed trial division

d669ee22305083dc0b519ef9f80d9dc298484a2a605d86bc1e8776b7b15cc3fe failed trial division f15862311efe2efed636ddca1b4eff8836cc6d9b98473f4f5ffc2b37bd5700a failed trial division

1b2f4b616ebed946026235b920b9024f4f4ed1dd382d9bfdc4b330ab5fd86dab failed trial division bbe44df80574d785da1e819ad8e45832a480c139a431bfecf4574fc679dcad3 failed trial division

ddab75e717c4dd4da244f5ab1a490abff3c58b7f3e5ebf584c06b205c1bc4f73 failed miller rabin bbb8b530fe28cf4119175dba6b37dd44e144b562cfb16a21bd9af2ed2550886a failed trial division

9dd74fe682eaabba0f2f0d785055d02b8f7566ddacbdd7dde971a98e92c8f512 failed trial division b5a49de4f0bc56443e26ab55555cc3b9a9105fffd95f92d7c48f28eda9f4635 failed miller rabin

4c1bbd052dda008ddf9856bc5ad312506cb1d352e2b8638bf22141fdc7acf96b failed trial division e1616b6a7a007e552d57b43c57465143d1890aca19519cd1508253e4c4aae74 failed trial division

9b6521cda783283cbfc46d227fdef4ea3df2c3351a8250104ab6534b0ec04cdd failed trial division
78f1fcd53c1a65aedf52fd1dc0e736700ea684369e026798501cb9c10e7fbcd5 failed trial division
5561dd14f2ef531088462f0fd92f0434bf5b6d433bdacfec66ac803abdc3f39d failed miller rabin
5cd9096cde933ff592fb6cefa7bcf16d56192fc27725670fdce51e0a9c928716 failed trial division
c147821ad7f29f2d754e66308295517ae8d94d2947022b8767a2e8abbbf3feaa failed trial division
d53c6f3bfe138effc943164edea303e30c966fdb326ec391baacadab49a7c946 failed trial division
ecac3b1a21fba559cb81dc1b831398fd33b498520b8dd70366dd8a3ca5c5e594 failed trial division
380eaddadf23f21baf482814ce15d8418c00f29692435274db8559dfda277d60 failed trial division
b46d7358f8bd104b3598c92505de3e2e050714b0e5614f5e1883247968375294 failed trial division
92d4a0fad9d319508efcf0d4963fb00f34fdd6c107a41d78fdf99c36f87cf59d failed miller rabin
714e38be6ccc592755e63c5a099e4db16bf6636ffda02681d3b8ad6e759af888 failed trial division
d81840addebf92d2ad813fb3ff8105d339923f2cb57e5c232da6dbc8526865f1 failed trial division
cdd9b2060bf7e0060fb61f6a08e0178ecf034c8a603be610fdf06b286364256e failed trial division
1c4f37b9f2c20bd2388e69f4bad25f9358e58033b16544e5912775324f52cdca failed trial division
2aa0bd425c7cab36d8401c13f0fb6ea87fcbd684fa618c3594c2be540ff4bd00 failed trial division
269aad666c1b7f518036c57e36f38cddb9280fc507d40cba0e8ccc3af384118 failed trial division
204aa533f4953a0ff7c489afb7dc924bc49e690e753a48680b825aaf0e419a4b failed trial division
da9ce268178b50987a9c4f58fd051882f1eebcbd2df66f853807eab50cde142 failed trial division
972fe2da2036b401338236925c5e6e9c0e17d0dcf6392efd87c42d781be772ec failed trial division
1181370dceb8932ae4084c45b83d290194049ccd48025f09c6f2ee66c56e240b failed trial division
a3fcc884683270b4dc8dbe2f157786aed4b2a9a6e02849c56bfd68bba75c029c failed trial division
6c49bf5ae5219910fa8a9cddf65308be33cc8645004006e5929dcbfaf9b1b8c failed trial division
38d50db1f22d86b3fc37460027af7db0274a15eef89a1103215f774b141f0c02 failed trial division
80112aa622790604092acfba63e703093425 91b88e94303ca3b63b784599bd2b failed miller rabin
4e4f7bdeae5803809b7de3491cf901ad758cdf4fedde9e54fdc1de52f750d59c failed trial division
d80b99da311372d8231665c9144575eae4d7c9c28448c51a82593449fe78089b failed trial division
2f6ac64fb324445a1fd51adc9272782d2a6b42126c633d851c0187dea38d9392 failed trial division
f6071b5429236b49e1a9f02bb6d94d9d2ad66ed4c2fde8d5ea872962ccd36d08 failed trial division
84628a0325d659fa68904ef4d646bed037dff83ecd87167a3d34ce257501cef7 failed trial division
39a95421c806103dbd4b583e7395c6da3fa16f82b71337c8106170374ad36fdc failed trial division
f64a36e31fc33c11233a9fe8703cf15902c78842f904998e873ab2ba9ebff87e failed trial division
8e493f828b3211fd576ed16fcd2fa6accc00d771cd3976b1f14b9682a20ec5db failed trial division
dea79707554df955ac39bf52a1e5b409c1b600f78e8a4ff03e03bfd949eb5b23 failed miller rabin
88572e4c3687d95534a56c460b1a1e9afabe43efaa990812959d8dc576329757 failed trial division
c254c1379965822573ecfb5a2d712a053d4cf530cad93a2749886deebe0011ef failed trial division
e826d1dc4f4edf4e7fd59ae51630f282bbc640ff2b049e4d37b4d992d4f77706 failed trial division
f664db86e45e61db83b7992f364511b508936dba77ca8687f5972f133f95e028 failed trial division
24cac6f2ba62a4444077027 65f6a4d6b548005896c330459f6898dbe41647fb6 failed trial division
18b6028516c01ced62af8f86bc4e679f5d77aad04c59ece12c6623a5f752a6ad failed trial division
6bd11b1c7984e7ddd55994e48759efbf500d9c764c3bd9b1b5d45c574b6f4d5a failed trial division
d6aa28e7bffac19e9bc7c5848fa5bef913b8a6a8637c8da1446892cfbcc8dc4c failed trial division
6456a3c671076b758a7614c4be57e55bfc0c41f30efdbf2049bc197d33d63dfe failed trial division
8ddc46c3ecf52db0e61a4d4da65e9696bc7cfdca3f5b85e445dd459f9998444b failed miller rabin
1faed7a84e900ae1fcdafceaeae3e613681736017b5ed3eac46c402a6648ca1e failed trial division
c3f90cbfe215733712e3dfe6935c90965c7a7217bd6b79d480e8f95c561713ff failed trial division
6c83fc3ee36e5e86438ef9af0cb21af5c93ef03725b4c145acfbe4e4699846a0 failed trial division
9ea722d36c57ea557c39683af81772fa3cc975042cf3e20761f2e4c1d3d85da3 failed trial division
718843a116137f5a8225e79412506c8efcb4e25872caad1931cc7e3e7c37fcc1 failed trial division
df60cf677485aaf3fa9836e7546fe00f11e209f842b1c2c24e2c0b5d88caa0dd failed trial division
ef73fd84f026cbe9311353999974c5567f88b99d84ed1a3e395a663ed1d6436 failed trial division
bcbc0e3646da951479c294b62c5aedae35270a8b7baa65ef8c0d52095d571d19 failed miller rabin
7bb3da5ab4133b73a62ec55bef2f1e612116513ea19c766144744d12c7bb8872 failed trial division
3680faac5e8c6bcd358dc0c364fefc7ab3677a9122386170ec9113d5ca1b9518 failed trial division
08b29dc4b29ce9e6cfeea3ecd3cd5f2b45e24ac0050d73a6f8185844a02c79e failed trial division
8df8d44d17eefcacc6c68b388ae4d6057aefad3a8c6e89e0ab6d3db513d71a04 failed trial division
f2de59cb48c5415d9aaf5259de17187b74c05b2d4337b59e3c27f38c18b46db failed trial division
5a9bf384ec14ea448c10106cd582b4464098921bf743bf139cd2d49a5f305f18 failed trial division
f92507eeb1f433bc172d81eedb70fdc6f7ec383433349b984c8a555b1cda04f failed trial division
b872985baada7f9e980b2cd0a1246995fbeaf81b06ac0f15cc679e1fd5870f43 failed trial division
8c1d56fbb34700b72239c03742cbf0c0afdb9be5070ed54e68937a4d63bb437 failed trial division
45f6d3bf4c4089de6ad200ea02ae5a0ababc0dd9b73578d579a011040c160e1c failed trial division
8285165277ee1aaeaa82383382be25392c431c460f3a60f69a5ebcd16d7fdc1 failed trial division
e9cdb079a391d827a8d51a6dcf5794d5669a73a1330dc6ee1f937996c7a2a53c failed trial division
ed7f2e479968eb066f3f026799366370423c2db2bc096fcd1e74048b106ff65 failed trial division
88aa0b131a131198ba422b657b5ddd791fc2e6836a0576a90dfd18a8439a80c9 failed miller rabin
41961331062b760fb4c8c5278df82a38283f8c7689230e2f675c87ffc7beac16 failed trial division
b06f9cd75cb755af56fc6306049672e99483e44150d9a431c86475f9b2cc050b failed trial division
9b3d92031adad404a096af2c15e2ed6bfe090ac793be5782e58426a757f8af6a failed trial division
75091fd238c7e0e277cc805131d46bba4bb5db81b5f9f3d3d2014d0ef6cdc54f failed trial division
5b0aa538c1ead52c1863c4704e942fe4ac54b14b8297d78d58330d3e9bb2527 failed trial division
7bfe56e9d6b8aa3875e4610f866abdc79943db2ef1aa9501a748b4567a873303 failed trial division
5a7f0ea0bd967818104424a89d8140bf3a2906e818f0a854ebedf73f37ccc82 failed trial division
ea42af1c3180d4d0546e5c82cc039ca5a7aff253fca58d1981e3adf9dc80f4dd failed trial division
30df440fa9f9aeec35691cc757da9e232af22a30ecef10ba63663920655bf655 failed trial division
af218771fb97d393882a54e300dc40ffe4b212edc139d85612d95baa3cbb1aa1 failed trial division
d19b260f1fb4fc50a4f90d15b627213d697e2137aa62035df23437503480f64 failed trial division
39b814a7b693c531e09b534cf7ead89e1dde000ac3a175c739c0e5d86d73746 failed trial division
dde48fb1b450907e5880f6450129956e7502b1e1a8390be9986fd95e33ebefad failed miller rabin
97bc2f5d972d49aa77efcc010876e6b6fcd745b08e34942aece5c65d75737f20 failed trial division
8c0e72a521670345c0b7b5fe8b73e563d50b851dfd8c88e7b17a321a95955a3 failed trial division
f9de98c5d935018d41e33ea680aa906fd9f339164c435d60f4c8794570aa77ef failed trial division
febc1c527056c3c566647a4ca8d283620926eb1999f265168e4a9c2e4a72661 failed trial division
cc9aac1d99aa6ae4067d22b9f7d5f6608471d9eda272654dd1e3cf6b7e9addfd failed trial division
579104d74f09b82ed445014d3814068a435ab82d124c46cc905261969c36995a failed trial division
2316e2de9d53b41a4ba7ce62c8550fba20061f2f8fa6be323456f2544716bde6 failed trial division
d81f51e25668972f01b013f2597abad5cb3a4cebfd0088ea7b5b1f92bdefba95 failed trial division
216302e6d9b6e74bdf3e36828ccac376924662d9139c3ef8111dcf81d8174d0e failed trial division
cb810f1431d8e77dd13b0df1b8bb9324ea637ea49c44af5b821bfaa3663d15d failed trial division
abc401d86cd343e96318374c0453ae85721a859eb5c5e4c3754f312e530a5455 failed trial division
4d245b2c1a300f847f93ca637ed2d089cb10a29b018b7d7765107a6ca8a18203 failed miller rabin
fefc4b9cceb48fb25f290f7c604047d0327cbb82a44f19c6098ecbb092a24775 failed miller rabin
2eb1e6074c452dddd0b25821426d7f1e0ef7b37e0ca0ffeb2116a52aba9db18b failed trial division
7b5d1abbb0a3c1d9f2d502f770a3ae79f93488290829f9f117f5e2f1ab41f1a6 failed trial division
5bb40070dd3d1b6994182dd9ca36c497b0fe12b6df1606e23d1256b22db9cf8f failed trial division
a57e3dde5c564506f1535de3662f3a7bbc03e71a4837a854d19913d7b3ed1f7b failed miller rabin
f9484f642eb4410b3ff637e5464078c4c76e2c768b72f157ce5cfe56e6d77f52 failed trial division
3195c3040f40ae6254fead32e1c982ed2f09897b7c64b1997cadcced2e0d9ef5 failed miller rabin
3734772d119fc4bf26605ab3777954b9774f51519d56591a10245d0832059f18 failed trial division
f25b6cca3785b040143c08dc3840c38d378aa4af70287ba17ffee900c8be5234 failed trial division
38586d50055dd622d4e299a74f93001c3d9d9b352e61477a77cd1725df382f3e failed trial division
7b35825cafb877ca965e6f23c0892e1354b347293c81c5cb5e31513e60900eb2 failed trial division
a552705ecf3518e558abb32f0671113a47afa2c3b5914a695c44d702cd33d9f7 failed trial division

b4c2040e288e1e56e0faef1850bedce02494740f0ebf3754b38cbdd7f2b52476 failed trial division 3ab68112a8a19af37a5f050b5df67304fa6a9ef426a7e7bfaef13dffaf49b4a8 failed trial division

7576844f08e4139b1aec2f65269a85063b0e32c08e26c46c692a1a90ecf0dbe1 failed trial division 90062816628222f8c0513942dc9278129551d61a51e9db978b85128895f93707 failed miller rabin

157486fbe65445a4d4777dacf55bbab8009180d142b88811d126cf23636b40ba failed trial division cdd186addf4af8d09271e5e7dcd24a992953c42742ec4b752d9d4431c632a6ab failed trial division

da8e9b5f40e1a4e8578fd4342bec019ee7f0a616c21905833d492fd49256dd42 failed trial division 7ff2decb5cdbe16915aa93856519f60bd39a231a8d92e851117fd2a1676eba86 failed trial division

9b3855f0fc6d98c752d036afd29f5cc7671b6b757e036580f39d60b1184596d6 failed trial division ab900ef6ab8d4b594525a18af472c9e5d53da335a988853c30d203f263b395ef failed trial division

fb6bafd3d0861c8b126e62bee79dd2d160038edcfd3ac5dbf76ff3a67cd03d3 failed trial division bbc7eda7034075e6ca64a94ab9c9d0bb194166cfb939ee18a850616ffd90915f failed miller rabin

9750e5952a08d8124891fa3457bb7c56bfa39a78cd883076d62f86df4ae0adf4 failed trial division 7093b213e76d9158192dea9b026080af0904125666e3852208399d82208613d3 failed trial division

27c3d1b13c295aa9cc5eba9807800606ed6f933ee7e52178bfe0644eb19f83c7 failed miller rabin 6eeab85ded1805d042f9feba7ddd3f29c5649a8d36fb3fe707b255c4c864ff55 failed miller rabin

b28b6166fd155725e9833cdfc78b71e8a7a91c87b1af3fb6e598cb49087e78e7 failed trial division 28ea27f44edc462a9f26b0b25cfb6ac9ffde63b560ced2f14958308287bac4e1 failed trial division

72174830516b1cb3e04687d2c4891499a1563f8aba8400aa15eeb3a2fdcfc238 failed trial division ad24a758e5562af6ac1bacbf1acff509d6794825e5b2fd382788ca9bd9a241f1 failed trial division

4e58741e5220e398fa3d19c5c41d3b28a97b61a8b777e6e9faabcbae842b7c10 failed trial division 6ff6eadfbe80654a0e0e2da4af757e27e54201f4b8c5d3d2080e9279af820c4c failed trial division

b1cd26e118ff83699b187daee23d5bc4b36a67aeac8a2d038ca39aa686f05e97 failed trial division 79e2175b675a7cbdbb4c664f53de15047e2313bc81c51bb529f4bbdb208780d1 failed miller rabin

547892ac90dd27cf6ee7878778d87b3b6463f9620f279d9bac519bbb0534bf3d failed trial division fe4c97c50ba99981b2d20b19d9f1ea1059383796c003d909129cf0107078fc6a failed trial division

42144aade684673f067e6861b7d06f93e4e5fe358a7434719811e811c95b54e8 failed trial division b1a5930300b74493063baf0c0ee2d20843c4091c3d547701c5c22600bbb20471 failed trial division

6a28c2a67c940663adb29848e8fd07425360de298f8d23dac038603e6268e1e0 failed trial division 2bec069014277ba40d340df6227c361421f5294a57aa351a7e4cb7992eb24af9 failed trial division

1c8087a950372648ef237c1cb2509c99b9d83fff4b32273eb45287ba8d1a9a9a failed trial division f8e3a387a52197e7c66187fcaadfb6401a8d3677e554ab7d97ce05f8b810208a failed trial division

72781161d62fae221e9b205f25f12d8beaac782b46adfa6fc8dac379c1cb9813 failed trial division 58c9f5fc7ccec965799297c50efd9a491e5ddd0184bbf18ee5815b8b1cfaa5b1 failed trial division

55d82fb7c495c05f5e024e16a47a1e2028e0bab6409c7b4a3ee905cc29daeba3 failed miller rabin 24a87c73dcf5a5ee9dcb7db33a27bd3921c02a4cc535a2263dba38f0cebd43d failed trial division

25190acfe0519fc3f229dfffa4b0cc5e1239978eac4b9406f1ae34ccc73fc9f7 failed miller rabin ab4f197ba3229580f1306c1a90300233639abe93a47d3a1b783c07e264001e46 failed trial division

9635836d78bc3aeb51ab9d1decf68b9de2c02e80455927cb9cc7b3369b00aa7e failed trial division 45b9f94cc053a791552d77fd4a8e44775ecc3f74c83804a0f0cdf0756c30be4f failed trial division

9e07c616162dddc0c27e1cd76a2a0a1885a029428a450d2d7ce3660700dca513 failed miller rabin 9608102e86bb0bc47685f25be6580f5c52246b6e36d2d2b168ece881617832bc failed trial division

2918a8f98fa7aceeb4c91479f0984d39ab5acd0b981674ae2241c5a0fceb923d failed trial division f4f7d96b09658d954480caa2709ee5f6d49450d9ea155cea6234b488f611f583 failed trial division

5813de622df1221e75040a3a6b8aa3665cdd4230bae8ad73b7ad16eeac86cc94 failed trial division af7a68aa4bed8f1b68e8fad37e746791e780e1a59cc0a613aa984a3c8c4b4e41 failed trial division

fd03ad30ded32c17df2850b3fcfc23036256ecfcafe0da10f69afd08fbbe99a1 failed miller rabin d5fb8e9db0c9f475aa7f5b8bd374f39e8373e1fcde03948d231164452580f989 failed trial division

b9ca603e792011d54623b88aca37e33bc851934189af6ba5a8e6e6ecfbd1b222 failed trial division 2cbf2f79a2a0a2dab5a559c1e62d8e0f19713a87ea57bc1b3dabd4c3865fa07b failed trial division

f9104fd9949043d51d50b6da51f98914dd5e0771dcb77ea8d205d9e0d2977170 failed trial division f498b613018d2672055bfe82e452dd13cf9e406ba8cf679e9aac69d3a3bf0c43 failed miller rabin

5a7cbd0bcae04939798616c33ae3fc4833fa27442a78703c791715cbc788d6e7 failed miller rabin c7bc6b60304d0e26a5d17ed28f001d7f8f5adb116095433b394028d1315f91e0 failed trial division

f9d9e07d0f47c1ad661a4b46b6afb95d2d83232e940e214549dd7f2543f357d3 failed trial division 18c060b632cb80c1656722a9ea3ff68aa3d776305046397cef45ebd831956f19 failed trial division

4263b773b1d1804089a43a292896baf1f4c4091f118dc10007bee8e2ecd12375 failed trial division 8297a9f21c76711e1aafb1da5db24bc407cf9e507da712ed25d77f905d5dae74 failed trial division

265d7c07fd3c96e3eb32a1311148cb42cf4f2bfc6828df0f2777e95d9dfdfe16 failed trial division 8fd271561046c84834d6d3f0f695c70732a2777eeb9aa5eb87e2494057c68533 failed trial division

51317cb15ee7ad3ad507505c4bd87130695a60699424b52659e73d94df35b0a9 failed trial division 4b1cd85ea61ffecae8398cc6a5ec788ff98cf45350ead684f0ed1397b3dbef2e failed trial division

66f1a34942d6231e6bfb21966da2665e8e96ec889d5d6b0e00ae3ae38f079086 failed trial division c3f31fe1257b834e9278d85803df700dc20e69e6d25d381d32294c216445582 failed trial division

e3212e9cce6e15d49a52c4b9e4fc67fafb6fc287aee54d5b207f8fbaa5c0a34a failed trial division f8f6dd4cab9ab6c922976a11adb1154680eaad9ca89c6dbd49cf1bc35637e566 failed trial division

d60207951245585b79362194c86d0ee8975bdb330bf449b4c05eeede0fd59fea8 failed trial division d0f156b8fb5ba54220669fa7f1932279e59a6046d3ba677dfaa97d3b38e096d1 failed miller rabin

62e5731cc2918afa1d7dc976bd76befe151e7f2e98bc4966f81baaa8164829c3 failed trial division fdbcd1c8fa6b97f7d9febad1acc46075c41e1ef5b881a52c40af349bb3dd90c8 failed trial division

46db15a4da2793397365ad9563222493253b63a53c7b6ff1e398d90fef5fca67 failed miller rabin d4894649626bf437b8e4743c2c248125702c5a098a5d0d42fc37b5f108cc7a8 failed trial division

e3458b1a60f267dcb3586b701140dc68a31acb6ad9d3585ebf347c87cdb00169 failed trial division 5015de8b075d487642ce9b51037866155e73a9148d01f26e43525cff9cb61520 failed trial division

1c4016f780c0cc599779d699fab1475fce6a3c092606eb0d675546580b3d5aef failed trial division 1035c9e22ade026a9b64de79dbaef1bfd8f039778b2f0d8f7fb3783c5b8bf468 failed trial division

8824e16161f59dbff565852b8c582d911a1e46a1e4948a9c06c25d02020ccfab failed trial division f27d3c4a4cfe3f37aae3d2a54041619a1d23b3b418f325875a21043f7ba18e57 failed trial division

4efe85998b3ac76f246047ec17cf7d79600a37ef11380900e257076de55c3fd6 failed trial division eb5bc874153fe8a128181e5571267141838e7b90f8f78e50a78264f688056773 failed trial division

75ae70681202fe1929b2665c974a00540d77134b97682e9f0197ed4524839ff1 failed trial division 1e7cd988516b3a06c6249312f543c2dcdcdc680f3922aa6b5d6d4bdaa89023e9 failed trial division

7f755d83a840517c2c5afc9c2564192a0c6361932ac6e1a240bda0f27ad336c6 failed trial division 7210f045140d0f3da6e4552ef3c46a0dedc24132b1a466cf5509b72feea0de44 failed trial division

438218828703fcd9edf5af14f55973697a54e50521076d2755d4b70234c72073 failed miller rabin ebd76dcc75c9a7ccd7613848e9429bea9a3ef02d3d811a5f51cb8fa384e751a8 failed trial division

416508a743109c03f78bcf4223cea179cde31c6dc60a1eb17ede202ac659e957 failed trial division 8bbecde53689b7cf5902bafccb8e3e2a5250c32e495e3197c0296dae0062101d failed trial division

96c3ae5e91489843efcefd218ae25ace36e883073664d65d00a19f69a5ff6f3e failed trial division 7c73e1ed93bfdede30a28b3d795288168c164b2a3fd42c89dc103799f227e772 failed trial division

4765c52f25a65805a20f46459118ffd715b15b91aadc680fbf5995d787c2830b failed trial division 6e0127bcddcd17d9b29ebdd48a480e6a702cbb450a05eec70870a362a57ae41a failed trial division

4be75eb14a901f11b31324495bc0b61f27f30c3a7b945a54331b39defb17f4fc failed trial division 56725eb25afcf62823c568ca1f9c9e5fb27ac66c7bfd1542c52ac00bf4035e50 failed trial division

916f3ba164eb46eba4350cd44b74f7574bcb2fc1b8640dfb7128e14caf0c820b failed trial division 4865821368625**61c5ab8b45caae6f6d8b15ae0a5bc87c078ebfc58d06ba41943fb** **is pseudo prime**

8ea68f6b05b284c612b12b0bf0425e37875cd81794dbe371e74cb6a6b683f632 failed trial division

Key pair generated

```
**************************************************************************

Chris

Modulus:

213ba9040d54ac72ef4f82954f13fa067e40c722e262fba36b8c4f3e35091d12b708d47a06884f3234e13
7916715cbc01624ce91a8b260db104206e53ec4a81

Public exponent:

d56c5f2934ce0702c38f1e7f0d9c875ba14846f742d7835162a9af1b93a92917

---------------

d:1df7710328604a41bee6bb89b8a0a87ecc63ec4bd20e08529a091cdb0ecafd780cbef26f26e1f86c933
f8924795dccbeafc84ceee06ac8464b20104fa6242a7

p:3716b9f7fb50caa6b29262504aee73b811a26639491cfa8e2337e9e547f7a6b3

q:9a6f7a2bbabab2b9c7a631a63ce6ca87c8c5ec8a7076347fc58d06ba41943fb

**************************************************************************

Key pair generating...

///

c997ac737d8996743fc2ef6e6196629510262888c67b5f2809797631dd87fca3        is pseudo
prime

///

b9c892bea3e769a8ffbf7e779e1ce0767ccbd257f8c9fd1a56d21aeaf65534cb        is pseudo
prime

Key pair generated

**************************************************************************

Den

Modulus:

924c8daccff02a65a09ff2b87796b5df5846a4a9dc1b206c9a8c0ea3144035122b552e24c15de90a707f9
e4263fdb4c224b586fc6160b5a2a66d9073ce457141

Public exponent:

8800b6251c9c5c3f191578c76bf930cad822ca0fc987d50f581fbea2237ee1d5

---------------

d:3cfe1ac230a281a17cd171d1d182a8823b8aa6f787cdca5f0a9d3e0bfb91e3267b36810d73410176734
bf14a7d542b9b895d88323b2a3525a9e817b9d69b5561

p:c997ac737d8996743fc2ef6e6196629510262888c67b5f2809797631dd87fca3

q:b9c892bea3e769a8ffbf7e779e1ce0767ccbd257f8c9fd1a56d21aeaf65534cb

**************************************************************************
```

Chris signes a message

Signing message...

Message signed

Chris` sign: (123456,
dde3ceeda2e93a672678fc98a6ad22180ba46c7cc3b7d53ccb14db08d5ed01db5448660cb04427d36b8b6
21f691b477117e4155ba7e2ec1a8aaa0cf3a894d7)

Den verifies Chris` signature

Checking signature

Message: 123456

S^e mod n = 123456

Signature verified

Chris encodes a message for Den

Encoded message:
1f2115ca09718050a9e3fdc331576f6185cc0faef818c456ef26fddef862484539c0285c892ed205025e5
a13445a27bd7644b47e4bdf54ecaac3b25c849d931

Den decodes message

Decrypting...

Decoded message: 123456

Протокол конфіденційного розсилання ключів

1. Абонент A обирає ключ, який він хоче розділити з B

```
Chris sends key 21122019 to Den
```

2. A підписує цей ключ своїм секретним ключем

```
Signing message...

Signature for key 21122019:
108f1e1875155d184585cc56d60cd199b8daccf1731b419f9f4531e268d220b6ad8c819067c964914f695
5c759e00275bdd884b8cda7970bf4e5258e5dd95e
```

3. A зашифровує ключ та підпис ключа відкритим ключем B

```
Encrypted signature:
836c1ff792d1174f03b080381b25247dcf59ffc065325bbea4fae0616547cd54a47c0d437d33d70cb7b36
cf38bc8d22ca1e9ff3986ad0b3bd661a1271ec3e509

Encrypted key:
355d02d23dbc0345e9caa1866ac91a1f1181c62dea2e6edfd346429915b49e67bf53521c02c178a24b22c
86d6e5b65b8a46c2cf8f53779f07a39352baa7bd8dc
```

4. A надсилає B пару значень (k, S) по відкритому каналу

```
Chris` message:
(355d02d23dbc0345e9caa1866ac91a1f1181c62dea2e6edfd346429915b49e67bf53521c02c178a24b22
c86d6e5b65b8a46c2cf8f53779f07a39352baa7bd8dc,
836c1ff792d1174f03b080381b25247dcf59ffc065325bbea4fae0616547cd54a47c0d437d33d70cb7b36
cf38bc8d22ca1e9ff3986ad0b3bd661a1271ec3e509)

Den receives key
```

5. B розшифровує обидва значення своїм секретним ключем

```
Decrypting...

Decrypted key:  21122019

Decrypted signature:
108f1e1875155d184585cc56d60cd199b8daccf1731b419f9f4531e268d220b6ad8c819067c964914f695
5c759e00275bdd884b8cda7970bf4e5258e5dd95e
```

6. B перевіряє підпис ключата пересвідчується, що ключ прийшов саме від абонента A

```
Checking signature

Message: 21122019

S^e mod n = 21122019

Signature verified
```

7. Абонент B успішно отримав ключ від абонента A

```
Key recieved

Den received key 21122019
```