МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія
КОМП’ЮТЕРНИЙ ПРАКТИКУМ
Робота№4

Перевірив:
Чорний О.М.

Виконала:
Студентка групи ФБ-81
Ренькас І.О.

Київ – 2020

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

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

Порядок виконання роботи

1.Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.

2.За допомогою цієї функції згенерувати дві пари простих чисел p, q і 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента A, 1 p і q1 – абонента B.

3.Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p,q) та відкритий ключ (n,e) . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .

4.Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.

5.За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа 0 < k < n.

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

Хід роботи

Програма та всі її елементи створені так, аби працювати згідно RSA алгоритму, що описаний в методичних вказівках до Комп*ютерного практикуму 4

Так як, після написання алгоритму, його потрібно було перевіряти за допомогою спеціального сайту, при запуску програми, спершу потрібно вибрати буде це одинарна генерація ключів з цифровим підписом користувача чи програма створювати ключі та підписи для 2 локальних користувачів і надсилати між ними повідомлення.

Також я вирішила сторити 2 різні структури: PrivateKeyStruct та PublicKeyStruct – які об*єднуються в одну структуру KeyPairStruct, оскільки є певне обмеження на те, що функції мають приймати тільки

ті дані, якими буде оперувати, і тому передавати повністю KeyPairStruct буде порушенням цього обмеження.

Для перевірки натуральних чисел отриманих у програмі випадковим чином я вирішила використовувати Імовірнісний тест Міллера-Рабіна

Значення ключів для Боба:

p: 860855019260496175753872459385237463900003782061059370952012412401997180668 59

q: 935700277795627865180059596137095571474133068103723424375718901462360734167 03

n: 805502280663806848014106802325792826012667558001550206822077314913167433506962601516676425710414685558504754139060582566059399483473832782955472232134587 7

e: 498054187540082244845380849928591439686530256937272914846604018700513657667946024525073440204227497840257088722397898844378556410519570929792346143484607 1

d: 639495177573841488344261890677691031091701647899807809164355044359968405060293172955171612931717088458493990432471668878779453385398280036286793139015306 7

Значення ключів для Аліси:

p: 74573951365814344726051911897242794614702467025477004418815656932773156367329

q: 78478519701951626169660907817769613639357812999296783047942627292167423171643

n: 585245331151444343418659914567302073727624030438555789504783898234676723405418467280524511769807952503845538253429824732267618149772237561353820152445154 7

e: 312132604582848566800513635032051965462870538250642378817021033801989682193907264318699380713228201878840489332101274536549692897686493053012637579540628 1

d: 473267574580364635260396454628914846606923020000748780365934594544190220307249955519085268061128796829690275258559733752644568400033190224627637182092940 1

Числа, що не прошли перевірку на простоту, і причини, чому вони не підходять:

867219079842774113079251837667941908045198890949453786667756799494021874726 13 – не було вивлено чи є простим число чи ні, але ітерації закінчились

867219079842774113079251837667941908045198890949453786667756799494021874726 15 – подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 17 – подільне на 7

867219079842774113079251837667941908045198890949453786667756799494021874726 19 – подільне на 19

867219079842774113079251837667941908045198890949453786667756799494021874726 21 - подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 23 – подільне на 17

867219079842774113079251837667941908045198890949453786667756799494021874726 25 – подільне на 5

867219079842774113079251837667941908045198890949453786667756799494021874726 27 – подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 29 – подільне на 13

867219079842774113079251837667941908045198890949453786667756799494021874726 31 – подільне на 7

867219079842774113079251837667941908045198890949453786667756799494021874726 33 – подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 35 – подільне на 5

867219079842774113079251837667941908045198890949453786667756799494021874726 37 -

не було вивлено чи є простим число чи ні, але ітерації закінчились

867219079842774113079251837667941908045198890949453786667756799494021874726 39 -

подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 41 - подільне на 23

867219079842774113079251837667941908045198890949453786667756799494021874726 43

Iterations ended, p maybe prime, or maybe not

867219079842774113079251837667941908045198890949453786667756799494021874726 45

- подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 47

Iterations ended, p maybe prime, or maybe not

- подільне на 41

867219079842774113079251837667941908045198890949453786667756799494021874726 51

- подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 53

Iterations ended, p maybe prime, or maybe not

867219079842774113079251837667941908045198890949453786667756799494021874726 55

- подільне на 5

867219079842774113079251837667941908045198890949453786667756799494021874726 57

- подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 59

- подільне на 7

Testing 867219079842774113079251837667941908045198890949453786667756799494021874726 61

Iterations ended, p maybe prime, or maybe not

867219079842774113079251837667941908045198890949453786667756799494021874726 63

- подільне на 3

867219079842774113079251837667941908045198890949453786667756799494021874726 65

- подільне на 5

867219079842774113079251837667941908045198890949453786667756799494021874726 67

Iterations ended, p maybe prime, or maybe not
867219079842774113079251837667941908045198890949453786667756799494021874726669
- подільне на 3
867219079842774113079251837667941908045198890949453786667756799494021874726671
Iterations ended, p maybe prime, or maybe not
867219079842774113079251837667941908045198890949453786667756799494021874726673
- подільне на 7
867219079842774113079251837667941908045198890949453786667756799494021874726675
- подільне на 3
867219079842774113079251837667941908045198890949453786667756799494021874726677
- подільне на 11
867219079842774113079251837667941908045198890949453786667756799494021874726679
Iterations ended, p maybe prime, or maybe not
867219079842774113079251837667941908045198890949453786667756799494021874726681
- подільне на 3
867219079842774113079251837667941908045198890949453786667756799494021874726683
Iterations ended, p maybe prime, or maybe not
Testing 867219079842774113079251837667941908045198890949453786667756799494021874726685
- подільне на 5
867219079842774113079251837667941908045198890949453786667756799494021874726687
- подільне на 3
867219079842774113079251837667941908045198890949453786667756799494021874726689
x ^ (d * 2 ^ ri) mod p = -1, p - strongly sudo-prime
801305992654896432891158868716622986218816980495194025349930279726613140285 69
Iterations ended, p maybe prime, or maybe not
801305992654896432891158868716622986218816980495194025349930279726613140285 71
- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140285 73
- подільне на 7
801305992654896432891158868716622986218816980495194025349930279726613140285 75
- подільне на 5
801305992654896432891158868716622986218816980495194025349930279726613140285 77
- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140285 79
Iterations ended, p maybe prime, or maybe not
801305992654896432891158868716622986218816980495194025349930279726613140285 81
Iterations ended, p maybe prime, or maybe not
801305992654896432891158868716622986218816980495194025349930279726613140285 83

- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140285
- подільне на 5
801305992654896432891158868716622986218816980495194025349930279726613140287
- подільне на 7
801305992654896432891158868716622986218816980495194025349930279726613140289
- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140291
- подільне на 37
801305992654896432891158868716622986218816980495194025349930279726613140293
Iterations ended, p maybe prime, or maybe not
801305992654896432891158868716622986218816980495194025349930279726613140295
- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140297
- подільне на 19
801305992654896432891158868716622986218816980495194025349930279726613140299
- подільне на 17
801305992654896432891158868716622986218816980495194025349930279726613140301
- подільне на 3
801305992654896432891158868716622986218816980495194025349930279726613140303
- подільне на 97
801305992654896432891158868716622986218816980495194025349930279726613140305
Not prime, can be divided by 5
801305992654896432891158868716622986218816980495194025349930279726613140307
Not prime, can be divided by 3
801305992654896432891158868716622986218816980495194025349930279726613140309
Iterations ended, p maybe prime, or maybe not
801305992654896432891158868716622986218816980495194025349930279726613140311
Not prime, can be divided by 11
801305992654896432891158868716622986218816980495194025349930279726613140313
Not prime, can be divided by 3
801305992654896432891158868716622986218816980495194025349930279726613140315
Not prime, can be divided by 5
801305992654896432891158868716622986218816980495194025349930279726613140317
Not prime, can be divided by 31
801305992654896432891158868716622986218816980495194025349930279726613140319
Not prime, can be divided by 3
801305992654896432891158868716622986218816980495194025349930279726613140321

Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028623
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028625
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028627
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028629
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028631
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028633
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028635
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028637
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028639
Not prime, can be divided by 53
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028641
Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028643
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028645
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028647
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028649
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028651
Not prime, can be divided by 79
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028653
Not prime, can be divided by 71
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028655
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028657
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028659

Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028661
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028663
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028665
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028667
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028669
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028671
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028673
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028675
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028677
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028679
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028681
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028683
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028685
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028687
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028689
Not prime, can be divided by 67
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028691
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028693
Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028695
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028697

Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028699
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028701
Not prime, can be divided by 17
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028703
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028705
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028707
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028709
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028711
Not prime, can be divided by 19
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028713
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028715
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028717
Not prime, can be divided by 83
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028719
Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028721
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028723
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028725
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028727
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028729
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028731
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028733
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028735

Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028737
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028739
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028741
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028743
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028745
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028747
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028749
Not prime, can be divided by 19
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028751
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028753
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028755
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028757
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028759
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028761
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028763
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028765
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028767
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028769
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028771
Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028773

Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028775
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028777
Not prime, can be divided by 41
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028779
Not prime, can be divided by 47
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028781
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028783
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028785
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028787
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028789
Not prime, can be divided by 61
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028791
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028793
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028795
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028797
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028799
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028801
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028803
Not prime, can be divided by 17
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028805
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028807
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028809
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028811

Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028813
Not prime, can be divided by 37
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028815
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028817
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028819
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028821
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028823
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028825
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028827
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028829
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028831
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028833
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028835
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028837
Not prime, can be divided by 17
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028839
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028841
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028843
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028845
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028847
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028849

Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028851
Not prime, can be divided by 29
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028853
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028855
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028857
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028859
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028861
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028863
Not prime, can be divided by 19
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028865
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028867
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028869
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028871
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028873
Not prime, can be divided by 47
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028875
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028877
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028879
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028881
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028883
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028885
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028887

Not prime, can be divided by 37
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028889
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028891
Not prime, can be divided by 43
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028893
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028895
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028897
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028899
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028901
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028903
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028905
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028907
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028909
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028911
Not prime, can be divided by 59
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028913
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028915
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028917
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028919
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028921
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028923
Not prime, can be divided by 7
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028925

Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028927
Not prime, can be divided by 13
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028929
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028931
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028933
Iterations ended, p maybe prime, or maybe not
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028935
Not prime, can be divided by 5
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028937
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028939
Not prime, can be divided by 17
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028941
Not prime, can be divided by 11
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028943
Not prime, can be divided by 3
Testing 80130599265489643289115886871662298621881698049519402534993027972661314028945
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 29
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 31
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 33
Not prime, can be divided by 17
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 35
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 37
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 39
Not prime, can be divided by 13
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 41
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 43
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 45

Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 47
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 49
Not prime, can be divided by 7
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 51
Not prime, can be divided by 11
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 53
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 55
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 57
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 59
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 61
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 63
Not prime, can be divided by 7
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 65
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 67
Not prime, can be divided by 17
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 69
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 71
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 73
Not prime, can be divided by 11
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 75
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 77
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 79
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 81
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 83

Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 85
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 87
Not prime, can be divided by 19
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 89
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 91
Not prime, can be divided by 7
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 93
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 95
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 97
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365861 99
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 01
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 03
Not prime, can be divided by 79
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 05
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 07
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 09
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 11
Not prime, can be divided by 41
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 13
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 15
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 17
Not prime, can be divided by 11
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 19
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 21

Not prime, can be divided by 23
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862223
Not prime, can be divided by 29
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862225
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862227
Not prime, can be divided by 59
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862229
Not prime, can be divided by 31
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862231
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862233
Not prime, can be divided by 7
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862235
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862237
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862239
Not prime, can be divided by 11
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862241
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862243
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862245
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862247
Not prime, can be divided by 7
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862249
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862251
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862253
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862255
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862257
Iterations ended, p maybe prime, or maybe not
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862259

Not prime, can be divided by 83
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 61
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 63
Not prime, can be divided by 19
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 65
Not prime, can be divided by 5
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 67
Not prime, can be divided by 3
Testing 837748493843093227996104598231960120146507651895602859367130996093980365862 69
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254187 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254187 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254187 9
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254188 1
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254188 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254188 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254188 7
Not prime, can be divided by 41
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254188 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254189 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254189 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254189 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254189 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254189 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254190 1

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254190 3
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254190 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254190 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254190 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254191 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254191 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254191 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254191 7
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254191 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254192 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254192 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254192 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254192 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254192 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254193 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254193 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254193 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254193 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254193 9

Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254194 1
Not prime, can be divided by 23
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254194 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254194 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254194 7
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254194 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254195 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254195 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254195 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254195 7
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254195 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254196 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254196 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254196 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254196 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254196 9
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254197 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254197 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254197 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254197 7

Not prime, can be divided by 29
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254197 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254198 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254198 3
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254198 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254198 7
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254198 9
Not prime, can be divided by 71
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254199 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254199 3
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254199 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254199 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254199 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254200 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254200 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254200 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254200 7
Not prime, can be divided by 53
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254200 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254201 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254201 3
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254201 5

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254201 7
Not prime, can be divided by 43
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254201 9
Not prime, can be divided by 37
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254202 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254202 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254202 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254202 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254202 9
Not prime, can be divided by 47
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254203 1
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254203 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254203 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254203 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254203 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254204 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254204 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254204 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254204 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254204 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254205 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254205 3

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254205 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254205 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254205 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254206 1
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254206 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254206 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254206 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254206 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254207 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254207 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254207 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254207 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254207 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254208 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254208 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254208 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254208 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254208 9
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254209 1

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254209 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254209 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254209 7
Not prime, can be divided by 59
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254209 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254210 1
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254210 3
Not prime, can be divided by 43
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254210 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254210 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254210 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254211 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254211 3
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254211 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254211 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254211 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254212 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254212 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254212 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254212 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254212 9

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254213 1
Not prime, can be divided by 67
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254213 3
Not prime, can be divided by 41
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254213 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254213 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254213 9
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254214 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254214 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254214 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254214 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254214 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254215 1
Not prime, can be divided by 29
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254215 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254215 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254215 7
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254215 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254216 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254216 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254216 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254216 7

Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254216 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254217 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254217 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254217 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254217 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254217 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254218 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254218 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254218 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254218 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254218 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254219 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254219 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254219 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254219 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254219 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254220 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254220 3
Not prime, can be divided by 89
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254220 5

Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254220 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254220 9
Not prime, can be divided by 29
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254221 1
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254221 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254221 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254221 7
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254221 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254222 1
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254222 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254222 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254222 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254222 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254223 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254223 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254223 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254223 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254223 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254224 1
Not prime, can be divided by 37
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254224 3

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254224 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254224 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254224 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254225 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254225 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254225 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254225 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254225 9
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254226 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254226 3
Not prime, can be divided by 23
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254226 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254226 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254226 9
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254227 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254227 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254227 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254227 7
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254227 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254228 1

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254228 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254228 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254228 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254228 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254229 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254229 3
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254229 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254229 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254229 9
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254230 1
Not prime, can be divided by 97
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254230 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254230 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254230 7
Not prime, can be divided by 79
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254230 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254231 1
Not prime, can be divided by 47
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254231 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254231 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254231 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254231 9

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254232 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254232 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254232 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254232 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254232 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254233 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254233 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254233 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254233 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254233 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254234 1
Not prime, can be divided by 31
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254234 3
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254234 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254234 7
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254234 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254235 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254235 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254235 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254235 7

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254235 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254236 1
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254236 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254236 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254236 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254236 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254237 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254237 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254237 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254237 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254237 9
Not prime, can be divided by 41
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254238 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254238 3
Not prime, can be divided by 29
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254238 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254238 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254238 9
Not prime, can be divided by 37
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254239 1
Not prime, can be divided by 61
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254239 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254239 5

Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254239 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254239 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254240 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254240 3
Not prime, can be divided by 31
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254240 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254240 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254240 9
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254241 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254241 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254241 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254241 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254241 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254242 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254242 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254242 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254242 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254242 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254243 1
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254243 3

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254243 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254243 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254243 9
Not prime, can be divided by 83
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254244 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254244 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254244 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254244 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254244 9
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254245 1
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254245 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254245 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254245 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254245 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254246 1
Not prime, can be divided by 41
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254246 3
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254246 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254246 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254246 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254247 1

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254247 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254247 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254247 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254247 9
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254248 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254248 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254248 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254248 7
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254248 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254249 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254249 3
Not prime, can be divided by 23
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254249 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254249 7
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254249 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254250 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254250 3
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254250 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254250 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254250 9

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254251 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254251 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254251 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254251 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254251 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254252 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254252 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254252 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254252 7
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254252 9
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254253 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254253 3
Not prime, can be divided by 43
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254253 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254253 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254253 9
Not prime, can be divided by 23
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254254 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254254 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254254 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254254 7

Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254254 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254255 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254255 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254255 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254255 7
Not prime, can be divided by 29
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254255 9
Not prime, can be divided by 89
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254256 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254256 3
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254256 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254256 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254256 9
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254257 1
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254257 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254257 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254257 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254257 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254258 1
Not prime, can be divided by 13
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254258 3
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254258 5

Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254258 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254258 9
Not prime, can be divided by 31
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254259 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254259 3
Not prime, can be divided by 47
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254259 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254259 7
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254259 9
Not prime, can be divided by 17
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254260 1
Not prime, can be divided by 19
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254260 3
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254260 5
Not prime, can be divided by 5
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254260 7
Not prime, can be divided by 11
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254260 9
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254261 1
Not prime, can be divided by 7
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254261 3
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254261 5
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254261 7
Iterations ended, p maybe prime, or maybe not
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254261 9
Not prime, can be divided by 43
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254262 1
Not prime, can be divided by 3
Testing 6362154276652130769180890738670012685276636274692468937690113964372612254262 3

Not prime, can be divided by 79

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254262 5

Not prime, can be divided by 5

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254262 7

Not prime, can be divided by 3

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254262 9

Not prime, can be divided by 11

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254263 1

Not prime, can be divided by 23

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254263 3

Not prime, can be divided by 3

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254263 5

Not prime, can be divided by 5

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254263 7

Iterations ended, p maybe prime, or maybe not

Testing 6362154276652130769180890738670012685276636274692468937690113964372612254263 9

Not prime, can be divided by 3

Після того як ключі згенеровані відбувається виконання кроків протоколу конфіденційного розсилання ключів по відкритих каналах зв'язку з підтвердженням справжності відправника:

1.Користувач, що хоче відправити повідомлення(у нашому випадку Аліса), хоче надіслати деяке повідолення k

2.Аліса, використовуючи відкритий ключ Боба, зашифровує повідомлення k за формулою

$k_1 = k^{e_1} mod\ n_1$

3.Аліса, використовуючи свій секретний ключ, створює свій цифровй підпис S за формулою $S = k^d mod\ n$ і, використовуючи відкритий ключ Боба, зашифровує свій цифрвий підпис за формулою $S_1 = S^{e_1} mod\ n_1$

4.Аліса надсилає Бобу повідомлення (k_1, S_1)

5.Боб отримує повідомлення (k_1, S_1) від Аліси

6.Боб за допомогою свого секретного ключа розшифровує k і S за формулами $k = k_1^{d_1} mod\ n_1$

$S = S_1^{d_1} mod\ n_1$

7.Боб, використовуючи відкритий ключ Аліси, проводить перевірку цифрового ключа Аліси

$k = S^e mod\ n$

Результат проведення цього в коді програми:

Sended message from A

k1:
cb4ba68579f3051ee92778cdb07519a265f16f1a6aea8b7ea12bfc6c56b4456d2e346edcbcec5336c0fb76298ee
eda0eae02b37097c48aa2208445435c75ca4

S1:
35fc3bb130573efd1c68ac36aab789bb5991169cadd6eeb7875aab3a341a447f85e43fd766a8a5ca6b5caf158cf51e35754d3852e3be9eb23b673652853e428e

Recieved message to B

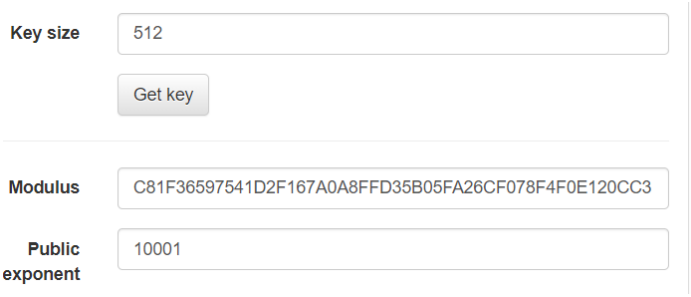
k:
3b98b951bec9dfd303c274a49d32718c7344f76658f9ad49732d41583623442714a7fad71e51783de7cf520923b02be4029ad8cf1f73622719dc790390a1b5c8

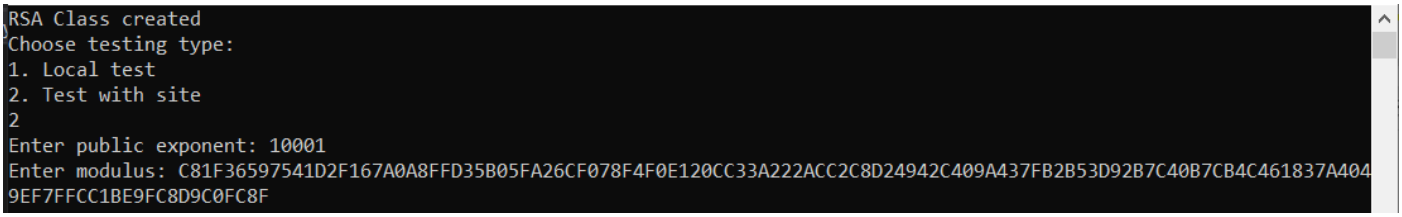
S:
2bf1463ff1035e09437c9fc4a03445b8ab54373380d8b62e47916c3d3c3eaf4e99423eddd04c63ae0b3f45664b3345efbbae16a4f52c551a90d2d4a8c290fee8

Data is decrypted properly!

Sign VERIFIED!

Перевірка коректності роботи програми за допомогою сайту:





…..пропускаємо момент, коли програма генерує і виводить всі значення згенерованих чисел, що не є простими

RSA Data:

p: 10334433116170310086892660923738237006610868540531442660453769070605530599117l

q: 7084403381168076455519982651809120156461142530604179816956823382569144219391 3

n:
732132929106522854393750056645636367685597249031033515527583889963830837924141195448922812773342907122467048971355393608409159125370102432752480924794212 3

e:
402962893167891891908378752934726195533120892856352155772301827503948744395865853902560244657212754670527285769335362463330549804161798168085877758544287 7

d:
106637272401359623118066133061479776222483174023594747801265674696611415198103954410551643366756461318093955438352330865215464993969607424751450297332709 3

Data for A

k:
4cf06a7a3c6b91a26fe47348f1d29ba38479edbb924f30ee1a9ca2040ddf5c79ad02a2af38f38327dd8d056fc73f57cdb8daadb0223342c9cc0c7fa3c703e03c

S:
707d38e42e2d1627c8537495dc89e466aa16b02c64a578431d710facb203393bb84625ccd268e1464727852845cc0577653eeb5769ec696863333ca1fac27849

Sended message from A

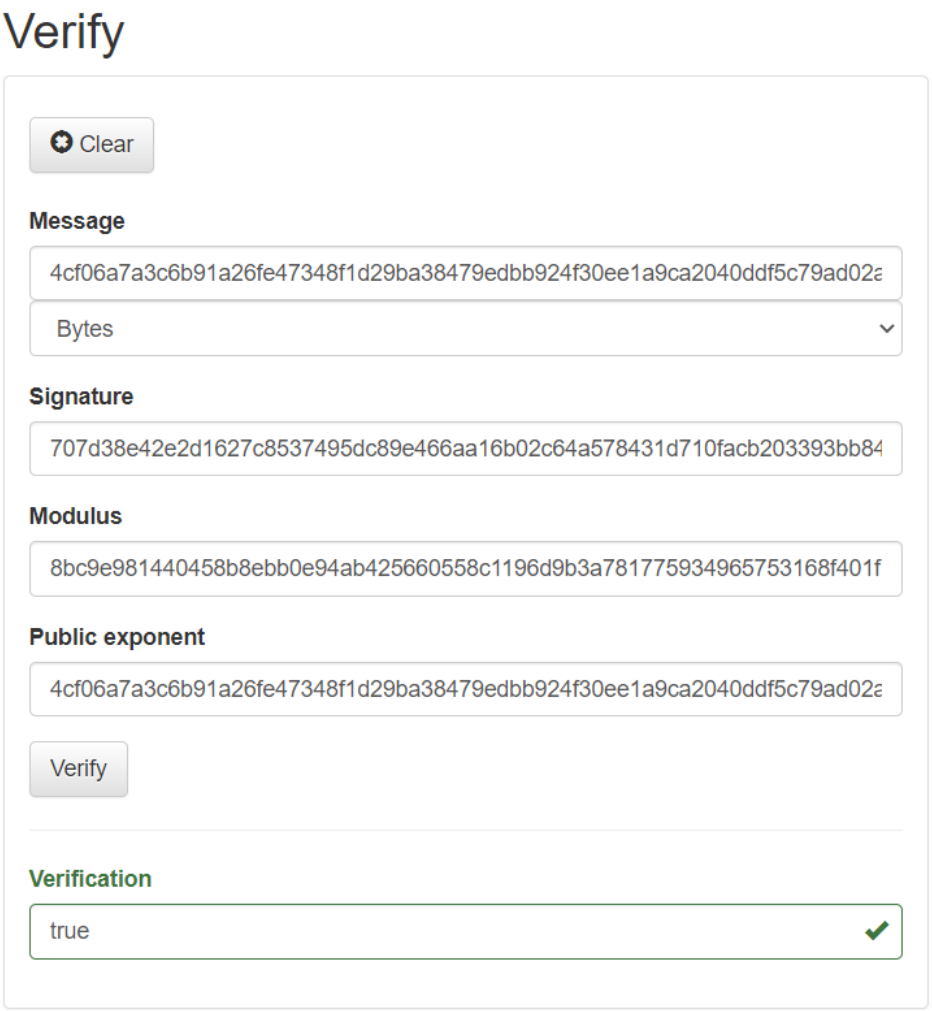
k1:
6dd6cad7e465d863172e1ab7b9b26dd9e6b49a95c20ccff63c06186bed107d1195bc6686c7a12ab758e75205ff799d4bfc079e1561b087b115c102778d946ba8

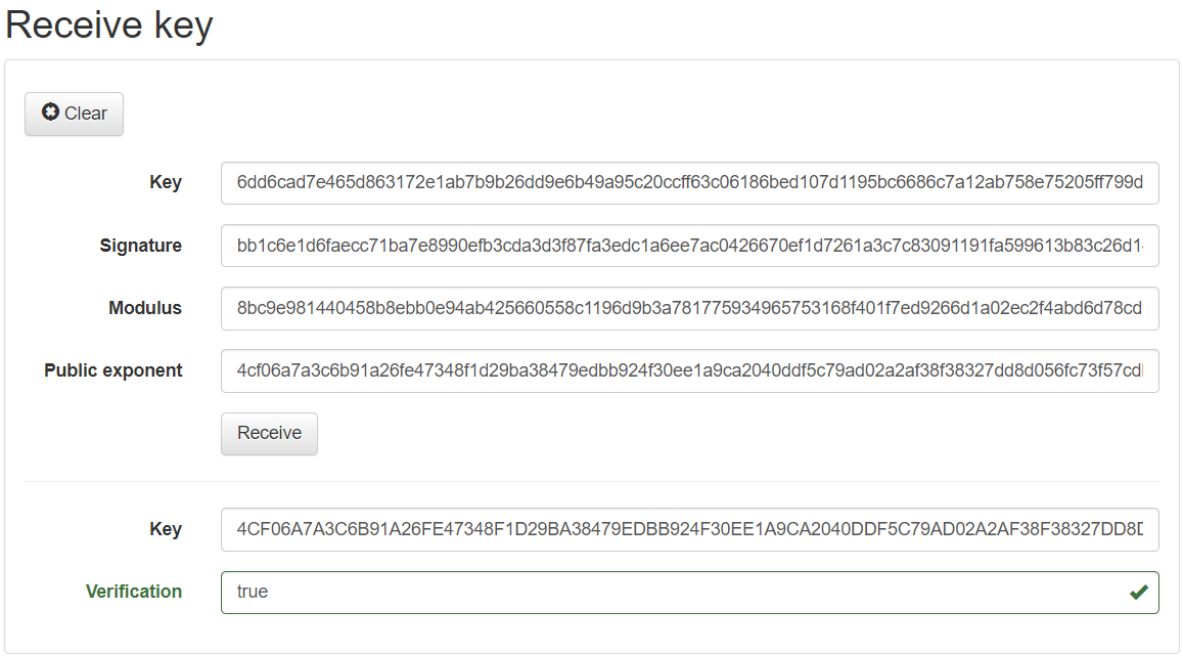
S1:
bb1c6e1d6faecc71ba7e8990efb3cda3d3f87fa3edc1a6ee7ac0426670ef1d7261a3c7c83091191fa599613b83c26d147e344473957b1680d35a2a51c5c65a91

Public key A: n =
8bc9e981440458b8ebb0e94ab425660558c1196d9b3a781775934965753168f401f7ed9266d1a02ec2f4abd6d78cd90c631332f0e41ddb7d09dba7bee8d9e5eb

e =
4cf06a7a3c6b91a26fe47348f1d29ba38479edbb924f30ee1a9ca2040ddf5c79ad02a2af38f38327dd8d056fc73f57cdb8daadb0223342c9cc0c7fa3c703e03d

Вводимо дані на сайті, аби переконатись, що все правильно





Висновки: під час виконання даної роботи я дізналась різницю між симетричною і асиметричною криптографією, вивчила основні пункти алгоритму асиметричного шифрування RSA та . імовірнісний тест Міллера-Рабіна на перевірку натуральних чисел на простоту та створила прмітивний код програми, яка в певній мірі демонструє роботу алгоритму RSA.