MATH4009 Project 2

Project By Sijan Malla & Ashmin Thapa

Objective : To find a large prime number

Our code for Program is

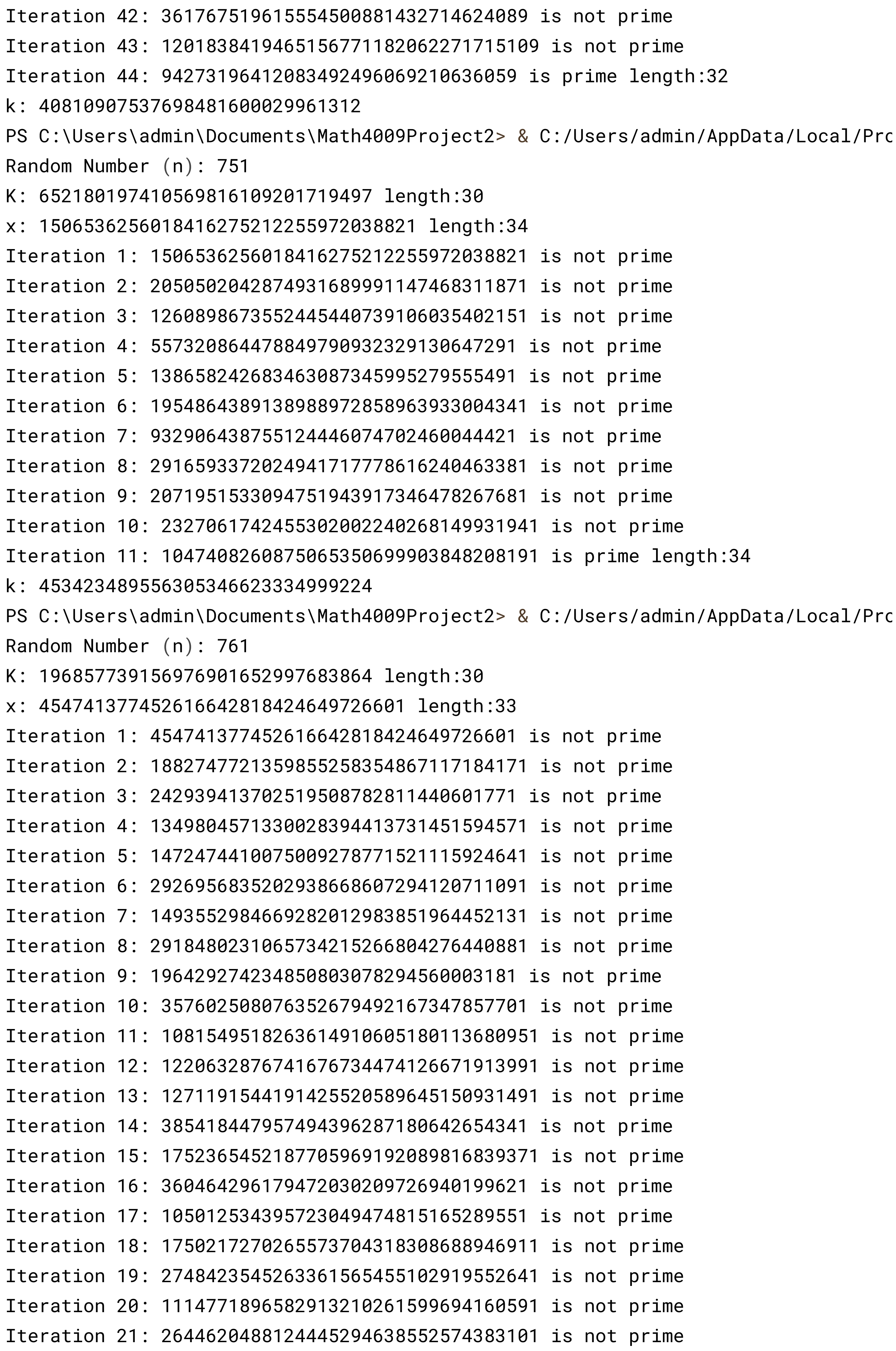
```
    import random

    # Making A General GCD function
    def gcd(num1,num2):
        if num2 == 0:
            return num1
        else:
            return gcd(num2,num1%num2)


    # 1. Picking a large random integer number in range of (1,10000).
    n = random.randint(1,10000)
    while gcd(n,2310)!= 1:
        n = random.randint(1,10000)

    print("Random Number (n): "+str(n))

    # 2. Picking a random integer K such that x = 2310K + n is 100-bit long
    K = random.getrandbits(100)
    x = 2310*K + n

    print("K: "+ str(K)+" length:"+ str(len(str(K))))
    print("x: "+ str(x)+" length:"+ str(len(str(x))))


    ### 3. Miller Rabin's Primality Test
    def MillerRabinTest(p,a):
okok9o9
        # Base case - 1 not prime
        if p == 1:
            return False
        # Base case - 2 is only prime
        if p == 2:
            return True

        # Base case - Any even number not prime except for 2.
        if p % 2 == 0:
            return False


        #Computes a^(n-1) mod n, using modular
        # exponentation by repeative squaring.
        m, k = p - 1, 0

        while m % 2 == 0:
            m, k = m // 2, k + 1

        x = pow(a, m, p)

        if x == 1 or x == p - 1:
            return True

        while k > 1:
            x = pow(x, 2, p)
            if x == 1:
                return False
            if x == p - 1:
                return True
            k = k - 1
        return False

# Method to call on Miller Rabin Test to check if number 'p' is prime or
# not with witness a.
    def isPrime(p):

        # 'a': a witness number between 2 and 'p' for which we check if it
        # is relatively prime to a or not.
        a =random.randint(2,p-1)
        if not MillerRabinTest(p,a):
            return False
        return True

## Driver To Run the Code and Find Prime Number
    flag = True
    num = 1
    while (flag):
        if (isPrime(x)):
            print("Iteration "+str(num)+": "+str(x) +
            " is prime " + "length:"+str(len(str(x))));
            print("k: "+str(K))
            flag = False
            num+=1
        else:
            print ("Iteration "+str(num)+": "+str(x) + " is not prime")
            K = random.getrandbits(10000)
            x = 2310*K + n
            isPrime(x)
            num+=1
```

2

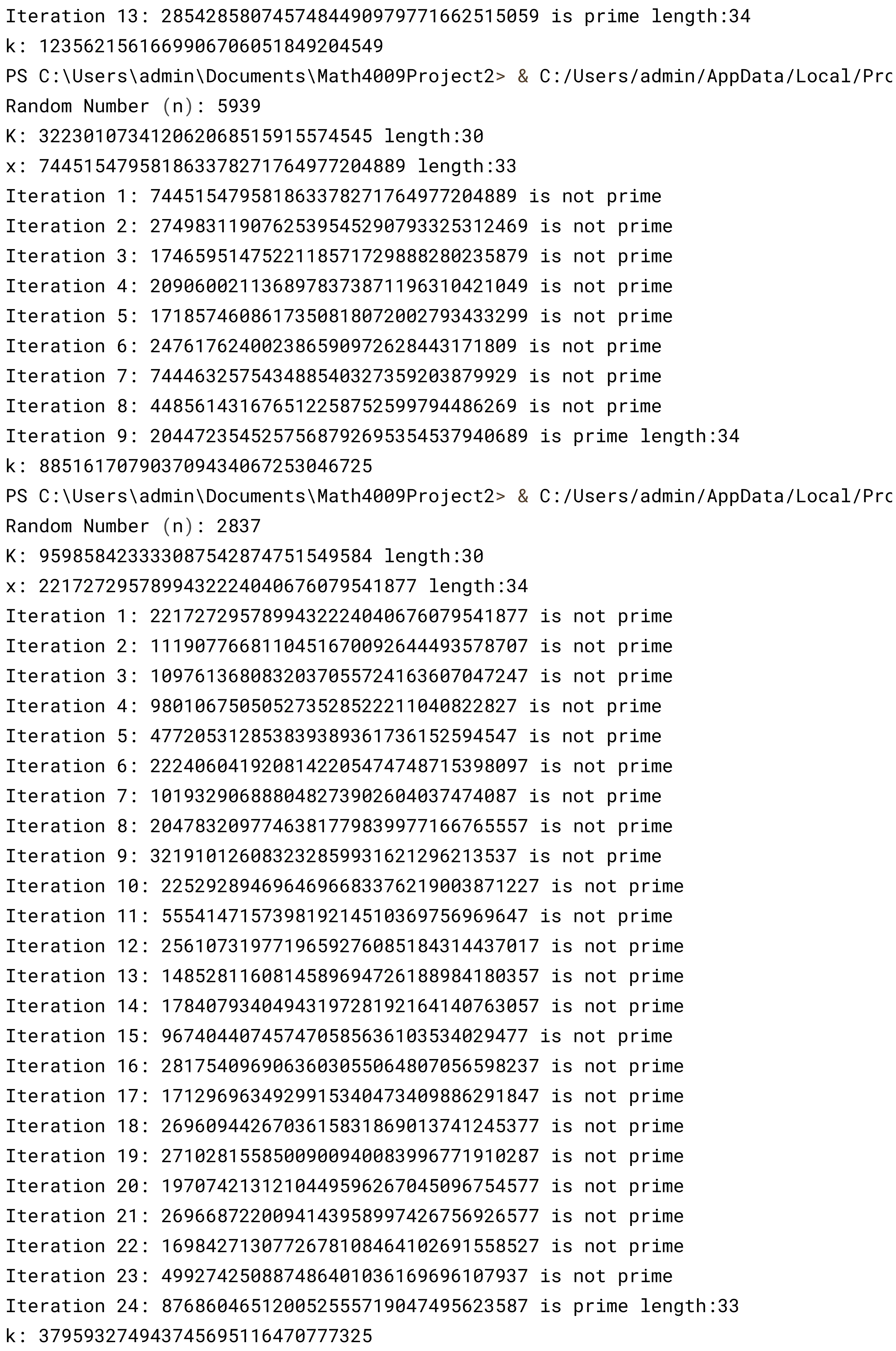
Ran Test Cases:

```
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 7463
K: 167082994916597671044396306851 length:30
x: 385961718257340620112555468833273 length:33
Iteration 1: 385961718257340620112555468833273 is not prime
Iteration 2: 1744039829283121937935530379944413 is not prime
Iteration 3: 862177548341557994308910955705353 is not prime
Iteration 4: 1207118922673326651325936118040053 is not prime
Iteration 5: 2740191632737638230351080185824513 is prime length:34
k: 1186230144042267632186614799055
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 3083
K: 413393107636655394172527982637 length:30
x: 954938078640673960538539639894553 length:33
Iteration 1: 954938078640673960538539639894553 is prime length:33
k: 413393107636655394172527982637
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 6331
K: 341831640665998253537654613864 length:30
x: 789631089938455965671982158032171 length:33
Iteration 1: 789631089938455965671982158032171 is not prime
Iteration 2: 519569165951206274652721281659521 is not prime
Iteration 3: 593748653813539008840820340625451 is not prime
Iteration 4: 2645104540171911207948524627706601 is not prime
Iteration 5: 2084828852609627527979074729645201 is not prime
Iteration 6: 2214583974024583372766987104050241 is not prime
Iteration 7: 2059903300217683636182578653074781 is not prime
Iteration 8: 2863919824323172729099942036058611 is not prime
Iteration 9: 1701050695622606730728362812035431 is not prime
Iteration 10: 1010424901851547991626606453659781 is not prime
Iteration 11: 358536224697909490218690991 37341 is not prime
Iteration 12: 936316355649618985471761239521861 is not prime
Iteration 13: 832742306191076430882094388074681 is not prime
Iteration 14: 1235324250971827104526890143724511 is not prime
Iteration 15: 2414088279352490786463343396090021 is not prime
Iteration 16: 1411153767858739218137502483502561 is not prime
Iteration 17: 454806723644355817237445299766041 is not prime
Iteration 18: 241132494464581655879513588330791 is not prime
Iteration 19: 291920741730474160685072920974301 is not prime
Iteration 20: 1496905480186920036059777707908091 is not prime
Iteration 21: 2417161635857092052383941731277511 is not prime
Iteration 22: 698238949088880647214224816327371 is not prime
Iteration 23: 2171198375956820720991550392282361 is not prime
Iteration 24: 636813314555617301245044809328361 is prime length:33
k: 27567675954788627759525749321 3
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 8359
K: 493333670508172176695208459494 length:30
x: 1139600778873877728165931541439499 length:34
Iteration 1: 1139600778873877728165931541439499 is not prime
Iteration 2: 1011281753193875483631436662489919 is not prime
Iteration 3: 2542416104331338532945357984925309 is not prime
Iteration 4: 2863548908354606209812317325569299 is not prime
Iteration 5: 1695011726992713176065852074427999 is not prime
Iteration 6: 1830742513986766088532174408361039 is not prime
Iteration 7: 2706901954979080906749345572473819 is not prime
Iteration 8: 2364964735893967843935436151071639 is not prime
Iteration 9: 2820984353266072963191736064423839 is not prime
Iteration 10: 2491104931080399935186104910373649 is not prime
Iteration 11: 584016855615488603432767138006939 is not prime
Iteration 12: 316655567562073632031473065296069 is not prime
Iteration 13: 2887539330641070888772246901669299 is not prime
Iteration 14: 1780390423493478212062770636482089 is not prime
Iteration 15: 1922926604077830898712718240170449 is not prime
Iteration 16: 2917017279256034435057185806165319 is not prime
Iteration 17: 2375314299878711780493058278237079 is not prime
Iteration 18: 259042972200447056694336622758289 is not prime
Iteration 19: 2274618557487254174097034649971729 is not prime
Iteration 20: 2735309488325962569666276808660219 is prime length:34
k: 118411666161297080937934060980 6
```

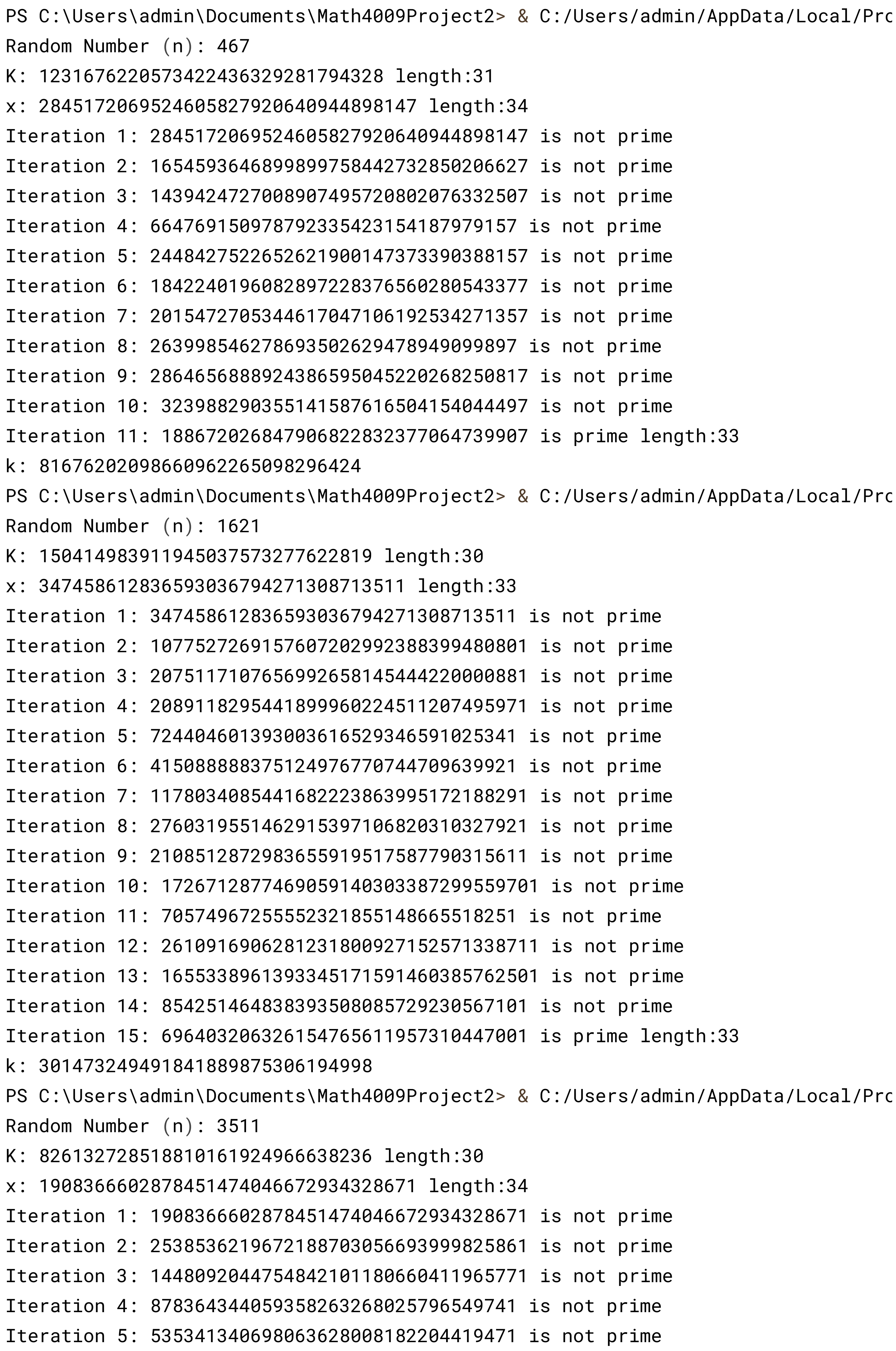
```
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Pro
Random Number (n): 5339
K: 276615485129995308247191454404 length:30
x: 638981770650289162051012259678579 length:33
Iteration 1: 638981770650289162051012259678579 is not prime
Iteration 2: 1324299773765317776498937647601769 is not prime
Iteration 3: 1640343870083502931345372160988689 is not prime
Iteration 4: 2731552597919644527673645124644469 is not prime
Iteration 5: 1435252870919546238397210780666439 is not prime
Iteration 6: 2032962953516965051468595291269559 is not prime
Iteration 7: 187369995109981337734591474906199 is not prime
Iteration 8: 2172220390944593954110792060937009 is not prime
Iteration 9: 334438590965779810686593852762969 is not prime
Iteration 10: 2325109131501437399121656900705099 is not prime
Iteration 11: 225353084596503638035604892420359 is not prime
Iteration 12: 2551089497539859974809572233782959 is not prime
Iteration 13: 657938202208212127508291881762739 is not prime
Iteration 14: 1496349207774416301062806177983419 is not prime
Iteration 15: 2570826229707614523087833624102279 is not prime
Iteration 16: 1463515268257467188797172669129549 is not prime
Iteration 17: 2506573001034553468560032204269889 is not prime
Iteration 18: 2734910625472485201993054748077929 is not prime
Iteration 19: 1478729463851290589823286352495879 is not prime
Iteration 20: 989656218059641792888286919531389 is not prime
Iteration 21: 1000619359175851069673713450018289 is not prime
Iteration 22: 2269343361909314423574913780159169 is not prime
Iteration 23: 721792881287976362360012452676459 is not prime
Iteration 24: 2069635143176314404365808630831899 is not prime
Iteration 25: 1704507823914535316651064820914749 is not prime
Iteration 26: 1410675701726118165888013104028799 is not prime
Iteration 27: 860639277810099630899420022758279 is not prime
Iteration 28: 118471725853558948801975026093599 is not prime
Iteration 29: 1724949699223110369105614942789699 is not prime
Iteration 30: 1238550765491667133668782523374189 is not prime
Iteration 31: 470441708250580965164006989472789 is not prime
Iteration 32: 1038448346748660690024755653251659 is not prime
Iteration 33: 1071119489466391305791558352835139 is not prime
Iteration 34: 1116699794181629513056254204378869 is not prime
Iteration 35: 411729566336302150055013163780229 is not prime
Iteration 36: 2421065869089564081589752065029769 is not prime
Iteration 37: 1068233910749395700670289023028499 is not prime
Iteration 38: 2111883601349792980763752787460629 is not prime
Iteration 39: 858087653348597169491625028152089 is not prime
Iteration 40: 1995293347922733704423079523960349 is not prime
Iteration 41: 2406427712080608172530789163489259 is not prime
```



```
Iteration 42: 361767519615554500881432714624089 is not prime
Iteration 22: 2838550956321783991813332593601191 is prime length:34
k: 1228809937801638091694083373853
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Pro
Random Number (n): 3139
K: 222450025930309369152010457664 length:30
x: 513859559899014642741144157206979 length:33
Iteration 1: 513859559899014642741144157206979 is not prime
Iteration 2: 2250380397253592001525906772617529 is prime length:34
k: 974190648161728139188704230569
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Pro
Random Number (n): 4099
K: 794589653318016017696401037654 length:30
x: 1835502099164617000878686396984839 length:34
Iteration 1: 1835502099164617000878686396984839 is not prime
Iteration 2: 2865013461753702502168787938372699 is not prime
Iteration 3: 1515473150448125846832534599941039 is not prime
Iteration 4: 241603932819745140239174301034639 is not prime
Iteration 5: 2455822224618185420662763451079129 is not prime
Iteration 6: 1357338432785373873109391210992069 is not prime
Iteration 7: 262637328129348731672752219841509 is not prime
Iteration 8: 879995299813369986539826597456949 is not prime
Iteration 9: 414779875139270393744416738256269 is not prime
Iteration 10: 870145123088224523320489392304639 is not prime
Iteration 11: 2833623759521571432664498530460429 is not prime
Iteration 12: 715391718060879679518514608449059 is not prime
Iteration 13: 762844369161768444016552141397899 is not prime
Iteration 14: 1957846994004886808310130905729409 is not prime
Iteration 15: 1760710030138681241295144587202949 is not prime
Iteration 16: 622427782606566399384527920627639 is not prime
Iteration 17: 321571410965217603370442349797959 is not prime
Iteration 18: 2041868180594698279351753532542099 is not prime
Iteration 19: 340840251365422539393072187416349 is not prime
Iteration 20: 512032437820082551037432471980909 is not prime
Iteration 21: 2460583582600376662129643935829239 is not prime
Iteration 22: 2598979198958848733519926439203909 is not prime
Iteration 23: 2158550408602367991716872526504209 is not prime
Iteration 24: 1555063664686053201339175630361419 is not prime
Iteration 25: 780421904784068027057804606526319 is not prime
Iteration 26: 1889537661683141192855239146805399 is not prime
Iteration 27: 878157420058001195464211158797439 is not prime
Iteration 28: 1230210757435846575653224824091939 is not prime
Iteration 29: 1457619029189034232128292531062619 is not prime
Iteration 30: 1639745343093176612548588535906029 is not prime
Iteration 31: 1046657566515345479324246496180319 is not prime
Iteration 32: 2757617846449685461096798774082809 is not prime
Iteration 33: 2274019430963063896490707002737389 is not prime
Iteration 34: 2546960298248720255401539355587289 is not prime
Iteration 35: 2355457021247987366252377507461499 is not prime
Iteration 36: 982317387969048674186968215913039 is not prime
Iteration 37: 1858459197883293700093557267811489 is not prime
Iteration 38: 2336682203802495046747234051648369 is not prime
Iteration 39: 1106760048752367459445534566218209 is not prime
Iteration 40: 381096943158908126137098633847189 is not prime
Iteration 41: 2018257256497576620453164218070569 is not prime
Iteration 42: 298905905984556433281523520935699 is not prime
Iteration 43: 1492855974705791319027280471773889 is not prime
Iteration 44: 2420607807070965574969885959423769 is not prime
Iteration 45: 1138499103019812052169497692025429 is not prime
Iteration 46: 1401954684123454397801229523298389 is not prime
Iteration 47: 15837501352183068870913197543349 is not prime
Iteration 48: 907617135252315878312200900914079 is not prime
Iteration 49: 89960752356039192244958866606099 is prime length:32
k: 3894404863897800530084799420 0
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 7243
K: 751796011731516326391877222911 length:30
x: 1736648787099802713965236384931653 length:34
Iteration 1: 1736648787099802713965236384931653 is not prime
Iteration 2: 551065550339285117722809338487223 is not prime
Iteration 3: 1004479698169610429781224997730333 is not prime
Iteration 4: 920663785461818611530034473384403 is not prime
Iteration 5: 1048674653990356052506091732692903 is not prime
Iteration 6: 1027497430194190351436201105976883 is not prime
Iteration 7: 1093313425991330947461255423592063 is not prime
Iteration 8: 2185860747174891157190439256927603 is not prime
Iteration 9: 1662013360880507020933965870218233 is not prime
Iteration 10: 477002719696766520626872799595073 is not prime
Iteration 11: 1248156238462895143676001100038343 is not prime
Iteration 12: 1212121219081474870045626858907033 is not prime
Iteration 13: 2414451971408231548816426610398813 is not prime
Iteration 14: 530226300503493734888152609260523 is not prime
Iteration 15: 1349461010705975301446466284398273 is not prime
Iteration 16: 1320218601066310359228249326324053 is not prime
Iteration 17: 2116684779458265227908472657246293 is not prime
Iteration 18: 1767634612308119482136657508143473 is not prime
Iteration 19: 2653296619277383458204054191324983 is not prime
Iteration 20: 1055916567912717847613908905489913 is not prime
Iteration 21: 2046662894554212818649312841369003 is not prime
Iteration 22: 1239267277843281134465295590926003 is not prime
Iteration 23: 1601119334509853641584416091941323 is not prime
Iteration 24: 4400026775289512776509402627913333 is not prime
Iteration 25: 12452525096772495227283118984035431 is not prime
Iteration 26: 17721047919264657967288440176467031 is not prime
Iteration 27: 26568865297089723743339185291097531 is not prime
Iteration 28: 21352703731322261803850133303510431 is not prime
Iteration 29: 29272233160429497065187759556036931 is not prime
Iteration 30: 25255224424890578122022265885102131 is not prime
Iteration 31: 13863765535679093826388827344017031 is not prime
Iteration 32: 27095762289910477922390102329115231 is not prime
Iteration 33: 5164561446879206895526056304207931 is not prime
Iteration 34: 7030683993404892040548205288560431 is not prime
Iteration 35: 13133126559695599870041840471163031 is not prime
Iteration 36: 363495162531062139426928412236031 is not prime
Iteration 37: 12398749745633644205619495601146131 is not prime
Iteration 38: 15551256545438963627887569224143931 is not prime
Iteration 39: 2514483692505609522438372288521531 is not prime
Iteration 40: 26543945783984085770337719359437131 is not prime
Iteration 41: 2280240982829686800374735287822331 is not prime
Iteration 42: 15939159189923467690044066540275231 is not prime
Iteration 43: 2539008200874345033215253538523831 is not prime
Iteration 44: 15526933567922060576156589136060931 is not prime
Iteration 45: 19886412672194700504388873929983231 is not prime
Iteration 46: 25169716860101876516010441323442131 is not prime
Iteration 47: 21402548495248649696771241548190131 is not prime
Iteration 48: 27324306149874492776662871841502631 is not prime
Iteration 49: 11407125204144799921086622528304231 is not prime
Iteration 50: 20470752414585211184325204685347731 is not prime
Iteration 51: 19577637453508416728571412740202031 is prime length:34
k: 847516772879152239332095789616
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 6869
K: 271779012426399821211116407040 length:30
x: 627809518704983586997678900269269 length:33
Iteration 1: 627809518704983586997678900269269 is not prime
Iteration 2: 2130205831961390737112005209454169 is not prime
Iteration 3: 488363504881366646166453535761599 is not prime
Iteration 4: 942893382791632762218715207923179 is not prime
Iteration 5: 2108191778275459498644378291365369 is not prime
Iteration 6: 2436416501598983019987749087177369 is not prime
Iteration 7: 2763082982527198974766502119767119 is not prime
Iteration 8: 710357575941894034804302238811549 is not prime
Iteration 9: 177923241018648048208101328456499 is not prime
Iteration 10: 2288196898639342314788039316140639 is not prime
Iteration 11: 2786960335427388682248591438471569 is not prime
Iteration 12: 890668163201164973755856685227669 is not prime
```

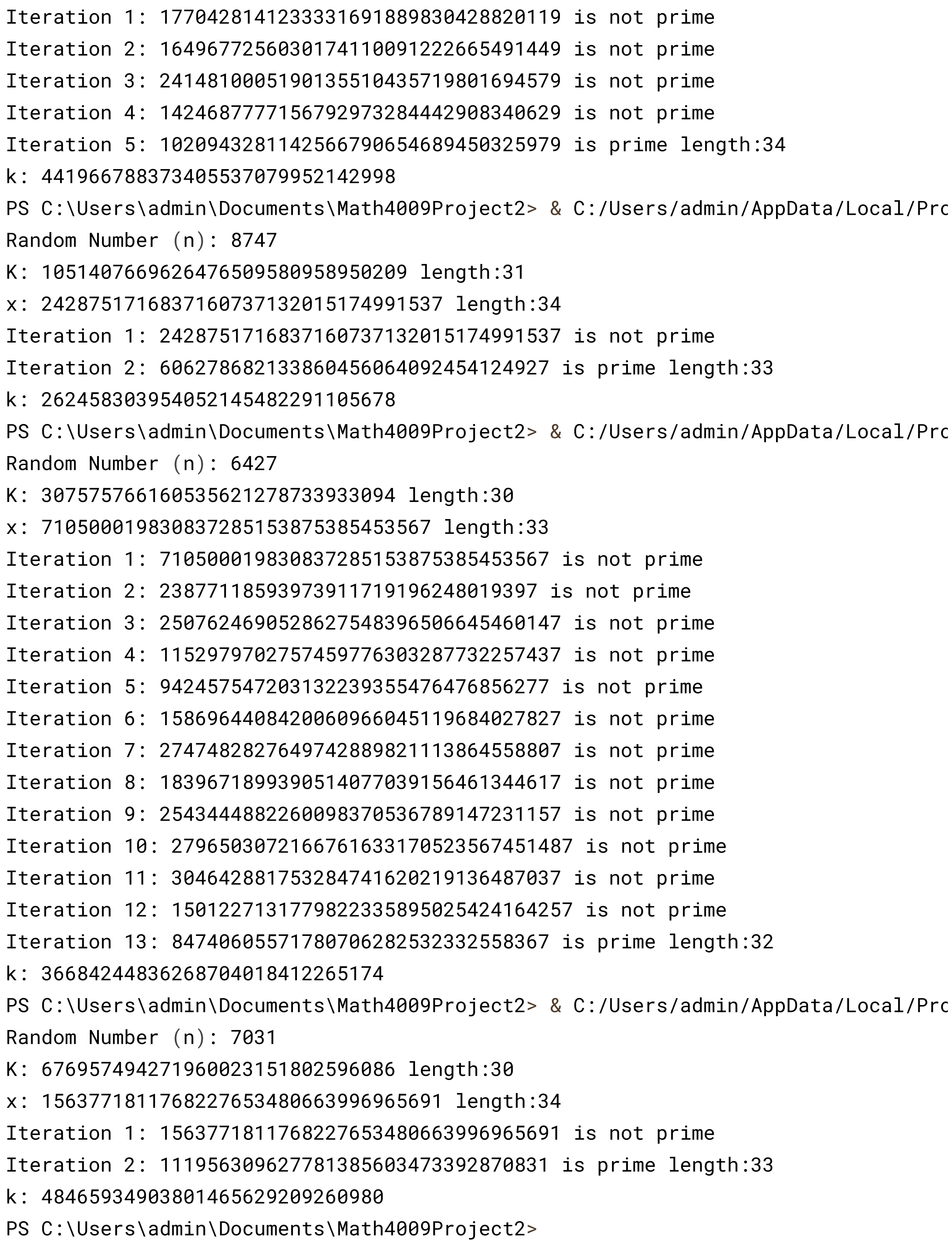


```
Iteration 13: 2854285807457484490979771662515059 is prime length:34
k: 1235621561669906706051849204549
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Pro
Random Number (n): 5939
K: 322301073412062068515915574545 length:30
x: 744515479581863378271764977204889 length:33
Iteration 1: 744515479581863378271764977204889 is not prime
Iteration 2: 2749831190762539545290793325312469 is not prime
Iteration 3: 1746595147522118571729888280235879 is not prime
Iteration 4: 2090600211368978373871196310421049 is not prime
Iteration 5: 1718574608617350818072002793433299 is not prime
Iteration 6: 247617624002386590972628443171809 is not prime
Iteration 7: 744463257543488540327359203879929 is not prime
Iteration 8: 448561431676512258752599794486269 is not prime
Iteration 9: 2044723545257568792695354537940689 is prime length:34
k: 885161707903709434067253046725
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Pro
Random Number (n): 2837
K: 959858423333087542874751549584 length:30
x: 2217272957899432224040676079541877 length:34
Iteration 1: 2217272957899432224040676079541877 is not prime
Iteration 2: 1119077668110451670092644493578707 is not prime
Iteration 3: 1097613680832037055724163607047247 is not prime
Iteration 4: 980106750505273528522211040822827 is not prime
Iteration 5: 477205312853839389361736152594547 is not prime
Iteration 6: 2224060419208142205474748715398097 is not prime
Iteration 7: 101932906888048273902604037474087 is not prime
Iteration 8: 2047832097746381779839977166765557 is not prime
Iteration 9: 321910126083232859931621296213537 is not prime
Iteration 10: 2252928946964696683376219003871227 is not prime
Iteration 11: 555414715739819214510369756969647 is not prime
Iteration 12: 2561073197719659276085184314437017 is not prime
Iteration 13: 1485281160814589694726188984180357 is not prime
Iteration 14: 1784079340494319728192164140763057 is not prime
Iteration 15: 967404407457470585636103534029477 is not prime
Iteration 16: 2817540969063603055064807056598237 is not prime
Iteration 17: 1712969634929915340473409886291847 is not prime
Iteration 18: 2696094426703615831869013741245377 is not prime
Iteration 19: 2710281558500900940083996771910287 is not prime
Iteration 20: 1970742131210449596267045096754577 is not prime
Iteration 21: 2696687220094143958997426756926577 is not prime
Iteration 22: 1698427130772678108464102691558527 is not prime
Iteration 23: 499274250887486401036169696107937 is not prime
Iteration 24: 876860465120052555719047495623587 is prime length:33
k: 379593274943745695116470777325
```



```
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 467
K: 1231676220573422436329281794328 length:31
x: 2845172069524605827920640944898147 length:34
Iteration 1: 2845172069524605827920640944898147 is not prime
Iteration 2: 1654593646899899758442732850206627 is not prime
Iteration 3: 1439424727008907495720802076332507 is not prime
Iteration 4: 664769150978792335423154187979157 is not prime
Iteration 5: 2448427522652621900147373390388157 is not prime
Iteration 6: 1842240196082897228376560280543377 is not prime
Iteration 7: 2015472705344617047106192534271357 is not prime
Iteration 8: 263998546278693502629478949099897 is not prime
Iteration 9: 2864656888924386595045220268250817 is not prime
Iteration 10: 323988290355141587616504154044497 is not prime
Iteration 11: 188672026847906822832377064739907 is prime length:33
k: 81676202098660962265098296424
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 1621
K: 150414983911945037573277622819 length:30
x: 347458612836593036794271308713511 length:33
Iteration 1: 347458612836593036794271308713511 is not prime
Iteration 2: 1077527269157607202992388399480801 is not prime
Iteration 3: 2075117107656992658145444220000881 is not prime
Iteration 4: 2089118295441899960224511207495971 is not prime
Iteration 5: 724404601393003616529346591025341 is not prime
Iteration 6: 415088888375124976770744709639921 is not prime
Iteration 7: 1178034085441682223863995172188291 is not prime
Iteration 8: 2760319551462915397106820310327921 is not prime
Iteration 9: 2108512872983655919517587790315611 is not prime
Iteration 10: 1726712877469059140303387299559701 is not prime
Iteration 11: 70574967255552321855148665518251 is not prime
Iteration 12: 2610916906281231800927152571338711 is not prime
Iteration 13: 1655338961393345171591460385762501 is not prime
Iteration 14: 854251464838393508085729230567101 is not prime
Iteration 15: 696403206326154765611957310447001 is prime length:33
k: 301473249491841889875306194998
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 3511
K: 826132728518810161924966638236 length:30
x: 1908366602878451474046672934328671 length:34
Iteration 1: 1908366602878451474046672934328671 is not prime
Iteration 2: 2538536219672188703056693999825861 is not prime
Iteration 3: 1448092044754842101180660411965771 is not prime
Iteration 4: 878364344059358263268025796549741 is not prime
Iteration 5: 535341340698063628008182204419471 is not prime
Iteration 6: 2285382219489012593273377270730251 is not prime
Iteration 7: 783337488589021244554453139574181 is not prime
Iteration 8: 2687736634789342442089179281009401 is not prime
Iteration 9: 2695222753983467349783639458715031 is not prime
Iteration 10: 1191521466086960728064721077224261 is not prime
Iteration 11: 548664810332310941904690358110931 is not prime
Iteration 12: 185959933415226576262579528256851 is not prime
Iteration 13: 70162450931090806719994079326471 is not prime
Iteration 14: 1420934877428656886010390597002281 is not prime
Iteration 15: 1100420408665830787121859894039541 is prime length:34
k: 476372471283909431654484802613
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 5167
K: 170932566581791303662002954677 length:30
x: 394854228803937911459226825309037 length:33
Iteration 1: 394854228803937911459226825309037 is not prime
Iteration 2: 215795793727455333433082190534547 is not prime
Iteration 3: 1220762606202251118815711266936657 is prime length:34
k: 528468660693615202950524357979
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 3907
K: 86221104601430454528226395025 length:29
x: 199170751629304349960202972511657 length:33
Iteration 1: 199170751629304349960202972511657 is not prime
Iteration 2: 835507573885479024050689728024907 is not prime
Iteration 3: 1820947663945422742472578079691427 is prime length:34
k: 788289032011005516221895272592
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 6583
K: 445696485865737042652350513235 length:30
x: 1029558882349852568526929685579433 length:34
Iteration 1: 1029558882349852568526929685579433 is not prime
Iteration 2: 809385409656385117501108069741873 is not prime
Iteration 3: 1902621568779934120240083446358373 is not prime
Iteration 4: 896394636988487858026278898907443 is not prime
Iteration 5: 2018670257795593854251196892234393 is not prime
Iteration 6: 761014045277381129732996519179273 is not prime
Iteration 7: 2403995682167311690651189938223243 is not prime
Iteration 8: 1533296221738520494065899460145273 is not prime
Iteration 9: 657223018894914937526078476842883 is not prime
Iteration 10: 2954168146652398687703574821627533 is not prime
Iteration 11: 1046643487258519895183996429511523 is prime length:34
k: 453092418726631989257141311474
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 5623
```

```
K: 1238940692514404990138763335268 length:31
x: 2861952999708275527220543304474703 length:34
Iteration 1: 2861952999708275527220543304474703 is not prime
Iteration 2: 1800125157075060932902620077592043 is not prime
Iteration 3: 1298896021697485993954442711933263 is not prime
Iteration 4: 2166306424331946822181099518565123 is not prime
Iteration 5: 720038882812043728504938890741143 is prime length:33
k: 311705144074477804547592593392
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 1217
K: 38196067469892220093105952321 length:29
x: 88232915855451028415074749862727 length:32
Iteration 1: 88232915855451028415074749862727 is not prime
Iteration 2: 936157508726813796893425786823747 is not prime
Iteration 3: 1954202467937421895535409903640097 is not prime
Iteration 4: 438241504861596557246888272010717 is not prime
Iteration 5: 1100360430643401419171547284821697 is not prime
Iteration 6: 1643226865753542857911347945140867 is not prime
Iteration 7: 2920328767692809728899788539678037 is not prime
Iteration 8: 1089654862881695701679447232423227 is not prime
Iteration 9: 1285823338468078294841905770266507 is not prime
Iteration 10: 21826138049019351763758195454517 is not prime
Iteration 11: 817528884770952025582685014567697 is not prime
Iteration 12: 781523028989980516976125717185227 is not prime
Iteration 13: 1624414710142365571416021080759237 is not prime
Iteration 14: 2071081057858410418039418318749307 is not prime
Iteration 15: 1836864132066939899371975426093487 is prime length:34
k: 795179277951056233494361656317
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 7177
K: 687098356415778785361148866803 length:30
x: 1587197203320448994184253882322107 length:34
Iteration 1: 1587197203320448994184253882322107 is not prime
Iteration 2: 1031345577694776224717223214461727 is not prime
Iteration 3: 1368325002609756195608199351187987 is not prime
Iteration 4: 2696097629588810160915174746210377 is not prime
Iteration 5: 1367116274993672800404066568571047 is not prime
Iteration 6: 1339857135882428268052109778196597 is prime length:34
k: 580024734148237345477103800082
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 5147
K: 116859803629730965378055814183 length:30
x: 269946146384678530023308930767877 length:33
Iteration 1: 269946146384678530023308930767877 is not prime
Iteration 2: 547664222768131526413746806775347 is not prime
Iteration 3: 2598728515602694309258520354093747 is not prime
Iteration 4: 500939845702225806788263964875097 is not prime
Iteration 5: 2864572392772251134294532587198657 is not prime
Iteration 6: 1090746964551377042301791236652957 is not prime
Iteration 7: 1663554583341131217358133422368677 is not prime
Iteration 8: 336465907321781742982612396627277 is not prime
Iteration 9: 2032503366722410186744378364276447 is not prime
Iteration 10: 1491633693705995676273713497600367 is not prime
Iteration 11: 2532830737056845121736054832484317 is not prime
Iteration 12: 6403059522309387747724341049096 97 is not prime
Iteration 13: 4832030000236657655970745206045 47 is not prime
Iteration 14: 1882295052209088836002406778065537 is prime length:34
k: 8148463429476575047629466571 69
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 8273
K: 1183651507087969085559033008401 length:31
x: 2734234981373208587641366249414583 length:34
Iteration 1: 2734234981373208587641366249414583 is not prime
Iteration 2: 1717009868751155731570267277999513 is not prime
Iteration 3: 674324503264018923585030005596463 is not prime
Iteration 4: 1321596649127714305000283212936463 is not prime
Iteration 5: 1479797414550610831082300553324083 is not prime
Iteration 6: 1103641571185481147302183338324413 is not prime
Iteration 7: 1575614558471652551587061884408193 is not prime
Iteration 8: 240723524332744783055772850556633 is prime length:33
k: 104209317892963109547953614956
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 9829
K: 1233475071350485762597896803875 length:31
x: 2849327414819622111601141616961079 length:34
Iteration 1: 2849327414819622111601141616961079 is prime length:34
k: 1233475071350485762597896803875
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 673
K: 732026653247347736943483390327 length:30
x: 1690981569001373272339446631656043 length:34
Iteration 1: 1690981569001373272339446631656043 is not prime
Iteration 2: 384946926506148886023821713109053 is not prime
Iteration 3: 1825430335824678188509734146365183 is not prime
Iteration 4: 1690470810843877989525104112566863 is prime length:34
k: 731805545819860601526019096349
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 599
K: 766419108759018048437156029792 length:30
x: 1770428141233331691889830428820119 length:34
```



```
Iteration 1: 1770428141233331691889830428820119 is not prime
Iteration 2: 1649677256030174110091222665491449 is not prime
Iteration 3: 2414810005190135510435719801694579 is not prime
Iteration 4: 1424687777156792973284442908340629 is not prime
Iteration 5: 1020943281142566790654689450325979 is prime length:34
k: 441966788373405537079952142998
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 8747
K: 1051407669626476509580958950209 length:31
x: 2428751716837160737132015174991537 length:34
Iteration 1: 2428751716837160737132015174991537 is not prime
Iteration 2: 606278682133860456064092454124927 is prime length:33
k: 262458303954052145482291105678
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 6427
K: 307575766160535621278733933094 length:30
x: 710500019830837285153875385453567 length:33
Iteration 1: 710500019830837285153875385453567 is not prime
Iteration 2: 23877118593973911719196248019397 is not prime
Iteration 3: 2507624690528627548396506645460147 is not prime
Iteration 4: 1152979702757459776303287732257437 is not prime
Iteration 5: 942457547203132239355476476856277 is not prime
Iteration 6: 1586964408420060966045119684027827 is not prime
Iteration 7: 2747482827649742889821113864558807 is not prime
Iteration 8: 1839671899390514077039156461344617 is not prime
Iteration 9: 2543444882260098370536789147231157 is not prime
Iteration 10: 2796503072166761633170523567451487 is not prime
Iteration 11: 304642881753284741620219136487037 is not prime
Iteration 12: 1501227131779822335895025424164257 is not prime
Iteration 13: 84740605571780706282532332558367 is prime length:32
k: 36684244836268704018412265174
PS C:\Users\admin\Documents\Math4009Project2> & C:/Users/admin/AppData/Local/Prc
Random Number (n): 7031
K: 676957494271960023151802596086 length:30
x: 1563771811768227653480663996965691 length:34
Iteration 1: 1563771811768227653480663996965691 is not prime
Iteration 2: 111956309627781385603473392870831 is prime length:33
k: 48465934903801465629209260980
PS C:\Users\admin\Documents\Math4009Project2>
```

After Running These Few Test Cases: (Total ran 30):
We got our prime numbers in 13.6 Average Tries.

Prime Number Found Are:

1. 2740191632737638230351080185824513 is prime length:34
2. 954938078640673960538539639894553 is prime length:33
3. 2740191632737638230351080185824513 is prime length:34
4. 954938078640673960538539639894553 is prime length:33
5. 636813314555617301245044809328361 is prime length:33
6. 2735309488325962569666276808660219 is prime length:34
7. 94273196412083492496069210636059 is prime length:32
8. 1047408260875065350699903848208191 is prime length:34
9. 2838550956321783991813332593601191 is prime length:34
10. 2250380397253592001525906772617529 is prime length:34
11. 89960752356039192244958866606099 is prime length:32
12. 1957763745350841672857141274020203 is prime length:34
13. 2854285807457484490979771662515059 is prime length:34
14. 2044723545257568792695354537940689 is prime length:34
15. 876860465120052555719047495623587 is prime length:33
16. 188672026847906822832377064739907 is prime length:33
17. 696403206326154765611957310447001 is prime length:33
18. 1100420408665830787121859894039541 is prime length:34
19. 1220762606202251118815711266936657 is prime length:34
20. 1820947663945422742472578079691427 is prime length:34

21. 1046643487258519895183996429511523 is prime length:34

22. 720038882812043728504938890741143 is prime length:33

23. 1836864132066939899371975426093487 is prime length:34

24. 1339857135882428268052109778196597 is prime length:34

25. 1882295052209088836002406778065537 is prime length:34

26. 240723524332744783055772850556633 is prime length:33

27. 2849327414819622111601141616961079 is prime length:34

28. 1690470810843877989525104112566863 is prime length:34

29. 1020943281142566790654689450325979 is prime length:34

30. 606278682133860456064092454124927 is prime length:33

31. 84740605571780706282532332558367 is prime length:32

32. 111956309627781385603473392870831 is prime length:33

3

In general it is assumed that the amount of trails of the test increases the chances of a correct answer. 6 is safe enough for all practical purposes.
According to Bruce Schneier in "Applied Cryptography", the chances of error for a 256-bit number with 6 trials are less than one in this is very low.
For our problem to find a 100-bit long prime number of form 2310K + n, I didn't find any prime numbers that were tested againts to be composite.

4

Finding strong liars: For our test cases of 30 we tested against the online Prime Number Checker.

5

If we want to secure our cryptosystem it is important to pick a random K and n. If we don't pick random numbers, it is easier to break the cryptosystem as there are only so many prime numbers that can be generated from non-random K and n. These numbers are important since they are used to generate keys for encryption and decryption of our private messages.

6 : Going Extra For the Largest prime number

```
Iteration 2700:
27527728965175257795016752968854078879404311395849458617369801066906246
12671738177028680268369628040240560040227287691486820474152969113350253
43592355434223628310640050688576807651951345266301708863029198854434845
17790529961373530960897742741280266992110424463698690753896615475280354
45037073231660479252738435856961280644531646974198138411391376798497894
45861606686293005446698503364372060827904060322569822443473195485443815
56682367406921548588645811750881226701961791510104599214061516735379984
42432707645553755645144660406982633967046967008948128321709800803023043
17577458323803879126590556033069413078500490330850730089949824892964802
74576081792915134265842257071513684474026223936199896374427875416065212
03344798540415650377136244504746833561674928143987503957123885052892657
18354790742834971977179871130865643686830544674851988138268767017191389
89114635495044168757621356949458111047794100541738903451564647995121848
18423558610841329380746774618560079406948070939205212799022147646081097
07028660118160576190796992985300394734798893197486702524204010622655815
24751214225516361915164950092540473226338381352633404674462316526775123
25873295444516218196467169184174372365304575607826381009759571701843326
60543788802315290128253043226217236810236032581768642222369283798283268
46242181391852000352551862163033117675300387912631362794836655652698538
57746045069253710928594512822637304295592464219413236699856362180196955
40946933590174826323200005338281410457264154193652618435442567370257818
50723084464928073105302351563642248610839654902541551546683858201789958
83208069765987145072438117350498111489693165518998840945594596386392556
22558105231467625855469434834721667616944692690236659920448225244568444
00215231847801239186379184207356831283988172648569659480259420357412805
```

31312920872987363072024721927841197130249324647369454016767590323547099
14388378984354038882164977862458968714436628890756884668481160330542429
01526340874342661047277957462597431496096268850032764242213969514206645
85289909365594970142696035792419839206216509474130961312818785787469569
27749148199497503555486042608819918399736086310671087063621284364985538
03976643701217191377135449907428100965927840790140283467062566503985270
95799333890473020020452823252935256024590369170793385196086809132102755
39243826043812523119088510123579741111895074846150787313943981040194161
24784921204894113819960942145029202026817081726417529250145995393182087
01842936083842034491084979262287731490352878327263279805893213835397372
78710252137869867326055677254883838965322732107722828064273600367704677
60190661129670113464514432615959087802506871426703007648790643313808084
18036797851163891163417883036462903148088152290753539950133122326233307
51888723747508418332545408946611904325930576668096803853670750594585624
25247751593277052729151504058583248462648530704290827399460958208787335
00640738332700782042305274766192888785992977375442338892557421885114373
75910303121341842388781793918001145846990200259270366695454796480303917
69144788941451904221937984528049 is prime.
length:3014

We had value for k:

11916765785790154889617641977858908605802732205995436630896017777881491
82974778431614147302324514303134441575855968697613342196603016932186256
89866820534295942991619069562154462186991924357706367473172813356898201
37571657991936593489566122398822626403511006261341424568786413625662491
10405659407645229113739582622061160452178202153332527450818777834847573
35870825405321647379523161629598294730694398408038884174663720989369617
12849509699966038350063121970078453117732377277101558101325331920077915
33520652660412881231664355154537936782271414289587934338402511170139845
53063834772209471483372535079250828172511034775260056315995595191759654
86829472637625599249282362368620642629448581790562725703215530483145113
43439306727452662500924781170886075134924211317743508206547136386533617
82837571750145009513930680143231880383909326699070124735181284423026575
71045296751101371756546041969462385734975801100319871624053960171048419
12737471260104471593396872129246787622055441965023901644598332314320821
24254831219982933415929434192770733651428092293284286807014723213270915

6915636979459582766890257579763656849625038153793653882011355693799788
8565943525736632822357886111869020448714483792546596580509072368045165
6539150600875823766788974213100507518659030444076920529101165730728498
9976728217052749783702403403533780570422207960135338252292137080369133
5664837491128539121685220541680633649536605734381792780809517591436372
1625718384993896860720013852836962257188126684650188972374179405053550
8996472174495439362802210087598079498808922441409048719286383845826061
3809345593422933592517102702948803051866298255115390432850257385047462
6143963734017771564794917123244306643816742930496505152539653335273702
3574391515244689111602268046051594894959667222505702445268250857255160
3278843313043849388441011388399338611594857018625511889496513160899029
8841362380581767874391143025463917653084237959802755969224055777785632
7287036468788539541504044442011808639594198022292682367467546651187105
6145083145653042853219289825547302858692312547151784264479399608714840
6400773796350336576399132023824915523993977575404327861845500740636639
0531790692014633756122814379736526898463163388788296938459216510945223
8366088761840999818152982271559308244710963330530563835080916484562129
7007276680563963373349896293560706143240303565280264553658332667319425
6014890954120959361378753768352430225091316945900087457496572175938324
3507125521182606437309218012287533960653029405293841190058566161353388
7361858534127877650557187238692077347731842758679150818031700138994471
1171613575773493708987095524298558490677278975158423847533552758193377
9253890868585774060970477783456760341608805968962617441694722430835097
5558419971048626075024899951185054148997110586185916068849895803362199
5532634358041151280762954652706317435953562403248510209198468679017620
9051200863467351553191926434663997086613941225336569965060120605756596
3394951901540009474075486475802178014466850167886553757580717952338529
2609106783353021492653849250712029844784374122051075551