**Московский авиационный институт**

**(Национальный исследовательский университет)**

**Лабораторная работа № 1**

по курсу «Криптография»

Студент: Фирфаров А. С.

Группа: 8О-308Б

Москва, 2020

**Постановка задачи**

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

**Вариант 0:**

n1=284994967805859272853477327862245466978346919806585432133556769 959269315271111, n2=588334127500298760075185369594470830068532538546945053004260193 945595259217406786089770982249290901568725608451508611541771305401 493870045176537915940249286141846560042142211542409633392281206603 637954450433183517707796541972311424681336480578342707287553065652 703205564979626673694073622920569912786167694946557747760150408914 919705012801904512377092934509169841743698528816250385854697524916 330387856905603362762198545848392715027208817212275244652775338978 6619

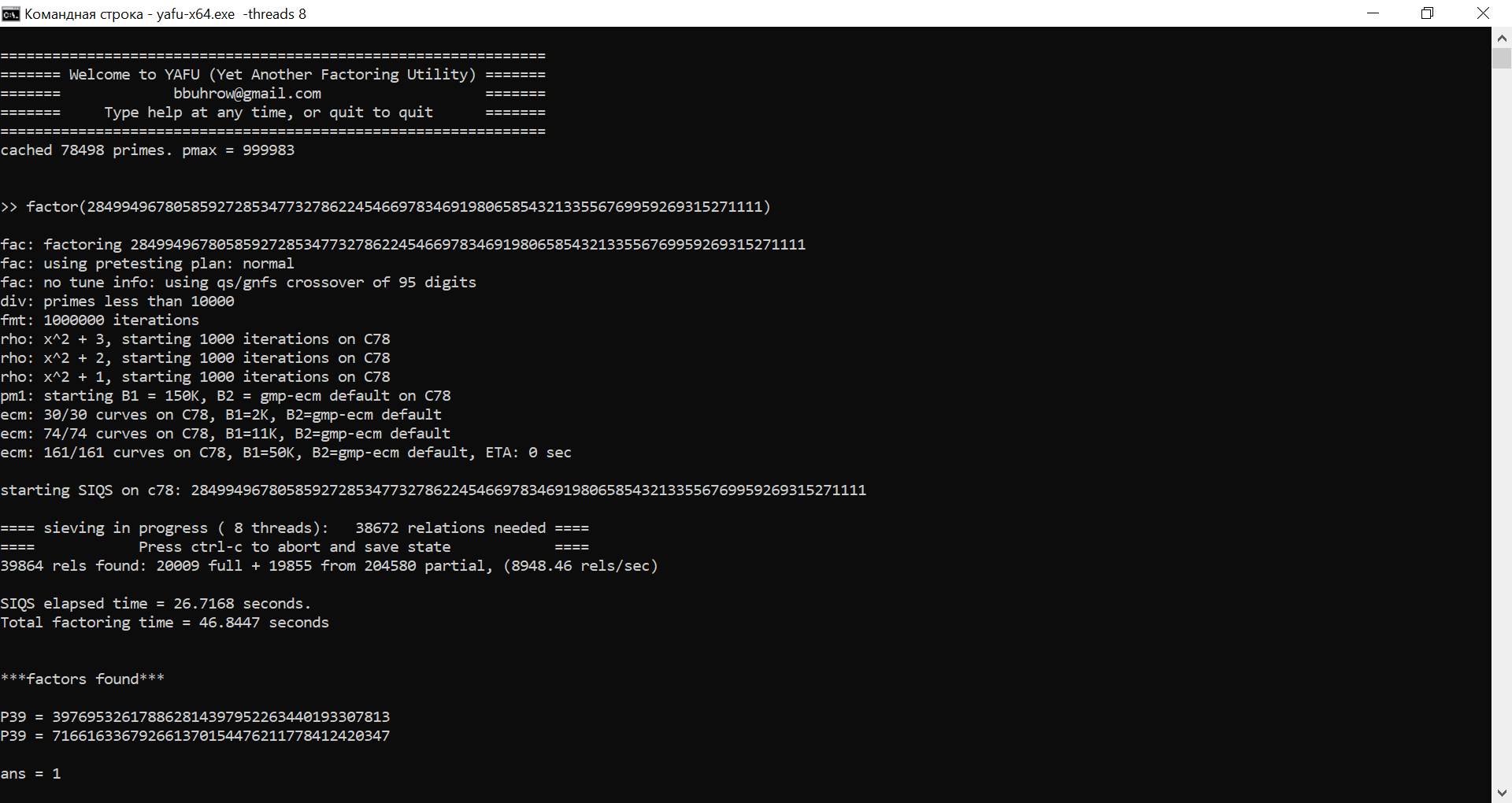
**Метод решения:**

Для разложения первого числа используется программа yafu.

При факторизации второго числа ищем НОД второго числа и числа другого варианта. Найденный НОД отличный от 1 и есть первый множитель. Второй множитель находим делением.

**Полученные результаты:**

Первое число:



Второе число:

div\_1: 338321131328863932564818680296074563081532769076856609725860402543148614331548252714137193761514829808776013335385989807884956317300479543405309911233314952878929489767681129617464167512042524219275287655118056649888395988512738187341200216598691518616681800731333973241210979683235278330374664946737167178077

div\_2: 17389813198762643193100409620078673760654183809100693115696916285733749398868672850488649953510095028267799834086695894233669398059248857067719029306421047

**Код программы:**

from math import gcd  
from sympy import isprime  
import time  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 start = time.time()

NUM\_2 = 5883341275002987600751853695944708300685325385469450530042601939455952592174067860897709822492909015687256084515086115417713054014938700451765379159402492861418465600421422115424096333922812066036379544504331835177077965419723114246813364805783427072875530656527032055649796266736940736229205699127861676949465577477601504089149197050128019045123770929345091698417436985288162503858546975249163303878569056033627621985458483927150272088172122752446527753389786619  
  
 NUMS = [  
 352358118079150493187099355141629527101749106167997255509619020528333722352217,  
 119760639583941053725652803731328419697649739176243841021915621242807618608591,  
 344845228130159226488163571070417679235025139015802019152516926202711846660141,  
 160769357899975610828199539114109518167531134514190990785144666932076614717841,  
 274114822339589629024026495441557479713813228028980117869052278950681241194819,  
 108762353292448487441247663685513658893167646930627178946128889967643172154127,  
 268887320029090028117214498253204095765884136483366193842361283776500643966781,  
 123248268911937923199906141216645363665087045422689358104089185316148911496103,  
 284994967805859272853477327862245466978346919806585432133556769959269315271111,  
 472379552736871494058143239162622860896965275113543450580272489891667080207763,  
 361996727456784871855604181056605672088622666207578160811291060873997151708887,  
 313230894596513941163065516500542159481861849753982064716706926040955753912601,  
 374456902508739435218273258671224457341348406488533188195528827819627513233269,  
 61121970174911146319545193754425119520875945215282784640177276523929376501913,  
 383456614884902466726252731294544234658015390619372835826246625499154384118189,  
 242587413455689311805941697582103544343444025737930609728129303011307601823551,  
 181552877565998943910618543225528579935321447209736978912489118450818545230489,  
 319373613270896663765954115654922624879359841665992852658124487372881123570003,  
 374456902508739435218273258671224457341348406488533188195528827819627513233269  
 ]  
  
 LARGE\_NUMS = [  
 4873822355066485648401071991924136818675872398286535454064775888224354057647759827888672904881758021952112721372792540754490030245608396182923905355014076090502386397665983839009222976102719595547524782591827859918063701352306472019393440971955164354386032725843607346843355546699218596423146704382946211873403241967325626024974089074590478580274181015361612573624846467079841362239862486328418954301422487721661475185724434860156652642467350107207026973065315203,  
 4640559218166094156914109159111519163187841151743307361441882837464585000644675874846465567321539765251799375820937589239985719737640895597242823431300043940827590777924614801336402643706476244259987080742848555919096958592308671421375157228642120372475705421693466178995623443185598183763791363779033266801228117576963439635390847153152534159364312454724658773080761415353568661089057964083886997037671005754984876814452951475039288901199175397709461135789384143,  
 3685159227155598432708028940420790505033167412889989029899886290757500906198848536416211136144358007549202044937915961098909838877993478676055552793938396505756737085059202486258700031418259779750808482075114707243226450683579197938892525246053563995434066959943535602408695367892174362462621739656937414835340145897293482734232981975633739612690654329902264503074506941004524051644869226017975806181694989764005951357225991720480110733573746714853210074207706721,  
 3508785995084440809528533987066115499570960157475289636203046237056172836433980089009328018596525578795975212269369781723178881963030441758416340899464309056072917227292230974069602435131842619562199965264459826662048705655605798421092322423487566587219114515580304022676070006294180033343897178565749085216188620723352965399425751141566775855490460717246126766384778691062473224303381227995700862458987531665489371414291536874311986532603244586962156742483483301,  
 4448469354559986526534775274117803974699059212231092249634001590040188264971159285942473071403768975120070026009479818278660862590363336881868724607727370461250222013516131492679992076856056258372426369392220537920803652608470269397938612736044388368307668164734539495822108219603207014929994653270346917309546127823781869069725331428314977499114078997620214362713623954104893108026744745661033981804357515124707435669786841955564937509542443636768031425380708233,  
 4721362061963649808863329010234613525807730599160259009967883741918385096173352581810523133667792305553466613259404177221188191288539451279983509237773260105978859945259643563529181076165441582984614364775297969359500787257106776187059853924659735017022670275642315020433647342524761924238275541410066296652437630661078222967549760189525938225926355453552756983354285083800596385481859173835256775993355195346250828163678329623000733278409956864037403335179310263,  
 4901462800240748416814014074841827076190073186231138227842097912957955878805324394488138207942891341407898651908158705529272793466722018916301658629323446920596326766419503621413621129013839104281727060865887110619779837584739827702346974784292078740174846408606944453368768724124418038303095193774022567738016084512349784513202034602912389469837957334750708492769061361926919741285735346263216442517251352648049433153722170396333395946227123813539207394201994703,  
 4204859705791455979586306353733656831387704289631337616530417253522871862141120631932433990091987949406971150143346271597491500705645949178093262134307318015307854194692933370809581210087664958072466290510175369552120495144991803400054486695900717370877845615837965857550517670683764602406916981979910029368736067741413430743475571851231332449065079917756805910750971996188143277035497059914480484135755951043475401544587782005555278233737918896409814525174854107,  
 5248627497522931463714873764259430511343970387129548219416937969810180441918139025234543071361527759234552973104202291837792918647457487910830237862019707673928761913941077209179901064097375908335106712169987969687036144095453438579278935837409458937553108352984618756366422619265155262955892256881506884138080346704519620186752439987072315479130627073733512177901387650465422163091473003309418048668930709969461093438389309285295556810281408328119130493934029969,  
 4502684846237985361154374235604838871670158677052705991602902830368307752162832875154089872181357405264220705933331329025365529514948135938279113805597028394835725879362660485184746760270328799312593533290859320294756303526816363798216162126316401690173022361808021178880238497414874854113701576932421403924657681536384091552364031299322735138829901806429292834343222064038278344385399530059140059091034110683488685728636107565148462358150648805006535015191878661,  
 4534841126241825968510749744330112537193576459685078508686505291277215984649118856625269593266314981908520149034604467171054282757028598783559627799693434744633779767712952142331753318472723319763577285804543416637427380566067189359748867034147472941880401619135051843062941005802021875588206859436303769445203798310577082473057060772111031984537886260745703434924863227606631371329108556798305647067089552901189288549521820753607107063151504851327159668098185307,  
 6935322526938199552538472490437575291803244940738234945475918435821368051484662276472561273504107781906830075394328076966980564652731377557949869817515416041455759125703317181079243557205769882044935450052309060331056934320287554780620005347843526382649902687943030117501100450883739213733484818337348392585796454790004245485859363365552338601237203357663127741515653465954857842494487929040401882928024088822429726706628046686893973455185139755966946831836312393,  
 6984851681366917241326658291520111481398796203245664950625456105855238488911928985954965545813417462798651076897976810194745304431137843084969470630248561233490765274509135725749751097268950654781344559124065033578802794544391711317414674364885693524784472926678187386421575006362139886189868057021545882889223084065171485872216788020836394215614336450313059634243461138994613485898295762404616754817834193145475466990768539491158574109125389062393262059696061591,  
 6523122455605210662166852670464123046410082552754972778516214048239779899959581220590625020743360492343073668835859391198224332970328529845480787899813683059854652628301127724670234965389517976093504678412536278942433021791526475133490313774653515165776970208025720935546643707581729280132057351527379825154329911856872332207538868730085883587106660609079956529803946773881720501869653418632220746434506343490085180086047883798335172360481853965007815045595021699,  
 7194132543632950834321278173504098007551907845600722577344402348276167868769953578598876714063677040246772381229540644061347416170512282794825375867434545931302351747173066239604467516142854736093749580275609060506138521951757085856066883166371115926918917029584965180268940087727797899902750423793915729868885808364246720390127172419974400639871071734663014297826772273362527587968331641899197048447253517730491262987083797926909288965170191454329430825696570851,  
 7081375258424870677512324321287877500122428328548362193252952718503087594397073442615147464815265010323649370021092433969727280717789710762303549515029836116642589113042769542300933516023826300033001137894122725052318253239085852046247380137571195085218519662340890924365075917370295331734045859329618008604551357279573925482053640034179561197570036076350877938633416918804454121061095381268851432072700370305583238840282914705414982154206911865475844097809295499,  
 5023285086821140763880680732713134774630698351035597979284186693310580016188513499920233361789635567176147515690925094958082677011319659422843361713526904401914379863383660265588900921137234927934954676282849419802761644394330673026415821404358521144952010424544812421730930886328673304556874295431061869419615441024117458299524133363461259040561309295442276237712457694313082340541549020944264139693933840715895581975093436871789164567620396191815924464955596449,  
 3850991093806146139466213576763072560323974056173842898999829203975658487705556063217434083007001013960865061736101114449098010377275426705821142177355593729229323449359675253896814654071267533503297560459670979497320466694278532459447601333939746092111856612610989088519675497962626035401516729815675734120153231706980856740092455544373459510039070031865293120630343053546824910219383508420681515780334893557343058853327025318143602405525566185899642616579670433,  
 4882319950398632503550205060580376494074805171565481495850372608210374184964449489619692851539489468336788354378812780486258607127873567402255468055188547212020945741021923365484007090416948014861065291209307404148989081722816917261980017993117943762750301367949002087916204288027696487069023936208662200539706807457696605647022113511537862912395207935843903788348410203770972758571105666943578913044252385537357054757874891705759713437611308764567920772879131189  
 ]  
  
 for num in NUMS + LARGE\_NUMS:  
 div\_1 = gcd(NUM\_2, num)  
 if div\_1 != 1:  
 div\_2 = NUM\_2 // div\_1  
 assert div\_1 \* div\_2 == NUM\_2  
 assert isprime(div\_1) and isprime(div\_2)  
 print('div\_1: ', div\_1)  
 print('div\_2: ', div\_2)  
 print(time.time() - start)  
 exit(0)  
  
 print(time.time() - start)  
 print('end')

**Выводы**

Основная теорема арифметики гласит о том, что каждое натуральное число имеет единственное представление на простые множители. Существует множество алгоритмов факторизации, но для разложения очень больших чисел эффективный алгоритм не известен. Этот факт используется в некоторых алгоритмах шифрования.

Факторизация первого числа не заняла много времени. Для факторизации второго числа пришлось найти НОД с одним из чисел другого варианта. Второй множитель быстро находится делением.