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=284994967805859272853477327862245466978346919806585432133556769959269315271111,
n2=588334127500298760075185369594470830068532538546945053004260193945595259217406786089770982249290901568725608451508611541771305401493870045176537915940249286141846560042142211542409633392281206603637954450433183517707796541972311424681336480578342707287553065652703205564979626673694073622920569912786167694946557747760150408914919705012801904512377092934509169841743698528816250385854697524916330387856905603362762198545848392715027208817212275244652775338978 6619

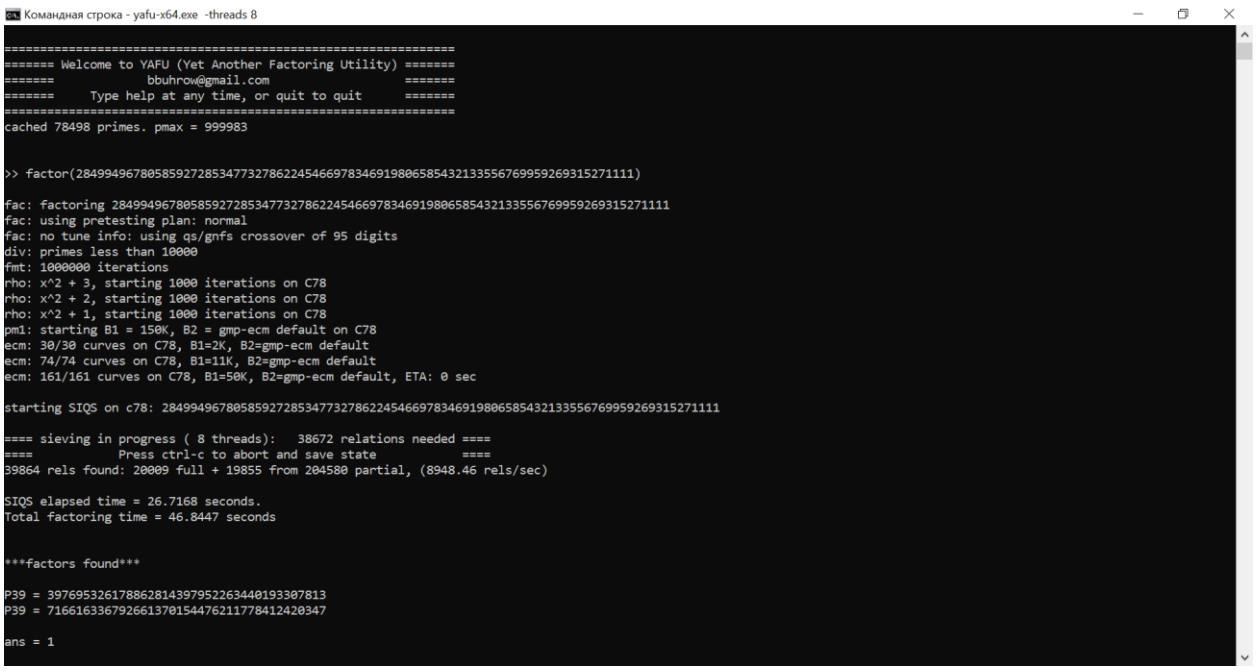
Метод решения:

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:
338321131328863932564818680296074563081532769076856609725860402543
148614331548252714137193761514829808776013335385989807884956317300
479543405309911233314952878929489767681129617464167512042524219275
287655118056649888395988512738187341200216598691518616681800731333
973241210979683235278330374664946737167178077

div_2:
173898131987626431931004096200786737606541838091006931156969162857
337493988686728504886499535100950282677998340866958942336693980592
488570677190293064210 47

Код программы:

```
from math import gcd
from sympy import isprime
import time

if __name__ == '__main__':
    start = time.time()

    NUM_2 =
588334127500298760075185369594470830068532538546945053004260193945595259217406786089770982249290901568725608451508611541771305401493870045176537915940249286141846560042142211542409633392281206603637954450433183517707796541972311424681336480578342707287553065652703205564979626673694073622920569912786167694946557747760150408914919705012801904512377092934509169841743698528816250385854697524916330387856905603362762198545848392715027208817212275244652775338978661 9

    NUMS = [

352358118079150493187099355141629527101749106167997255509619020528333722352217,

119760639583941053725652803731328419697649739176243841021915621242807618608591,

344845228130159226488163571070417679235025139015802019152516926202711846660141,

160769357899975610828199539114109518167531134514190990785144666932076614717841,

274114822339589629024026495441557479713813228028980117869052278950681241194819,

108762353292448487441247663685513658893167646930627178946128889967643172154127,

268887320029090028117214498253204095765884136483366193842361283776500643966781,

123248268911937923199906141216645363665087045422689358104089185316148911496103,

284994967805859272853477327862245466978346919806585432133556769959269315271111,

472379552736871494058143239162622860896965275113543450580272489891667080207763,

361996727456784871855604181056605672088622666207578160811291060873997151708887,

313230894596513941163065516500542159481861849753982064716706926040955753912601,
```

```
3744569025087394352182732586712244573413484064885331881955288278196275132332 69,

6112197017491114631954519375442511952087594521528278464017727652392937650191 3,

3834566148849024667262527312945442346580153906193728358262466254991543841181 89,

2425874134556893118059416975821035443434440257379306097281293030113076018235 51,

1815528775659989439106185432255285799353214472097369789124891184508185452304 89,

3193736132708966637659541156549226248793598416659928526581244873728811235700 03,

3744569025087394352182732586712244573413484064885331881955288278196275132332 69
    ]

    LARGE_NUMS = [

4873822355066485648401071991924136818675872398286535454064775888224354057647759827888
6729048817580219521127213727925407544900302456083961829239053550140760905023863976659
8383900922297610271959554752478259182785991806370135230647201939344097195516435438603
2725843607346843355546699218596423146704382946211873403241967325626024974089074590478
5802741810153616125736248464670798413622398624863284189543014224877216614751857244348
6015665264246735010720702697306531520 3,

4640559218166094156914109159111519163187841151743307361441882837464585000644675874846
4655673215397652517993758209375892399857197376408955972428234313000439408275907779246
1480133640264370647624425998708074284855591909695859230867142137515722864212037247570
5421693466178995623443185598183763791363779033266801228117576963439635390847153152534
1593643124547246587730807614153535686610890579640838869970376710057549848768144529514
7503928890119917539770946113578938414 3,

3685159227155598432708028940420790505033167412889989029899886290757500906198848536416
2111361443580075492020449379159610989098388779934786760555527939383965057567370850592
0248625870003141825977975080848207511470724322645068357919793889252524605356399543406
6959943535602408695367892174362462621739656937414835340145897293482734232981975633739
6126906543299022645030745069410045240516448692260179758061816949897640059513572259917
2048011073357374671485321007420770672 1,

3508785995084440809528533987066115499570960157475289636203046237056172836433980089009
3280185965255787959752122693697817231788819630304417584163408994643090560729172272922
3097406960243513184261956219996526445982666204870565560579842109232242348756658721911
4515580304022676070006294180033343897178565749085216188620723352965399425751141566775
8554904607172461267663847786910624732243033812279957008624589875316654893714142915368
7431198653260324458696215674248348330 1,

4448469354559986526534775274117803974699059212231092249634001590040188264971159285942
4730714037689751200700260094798182786608625903633368818687246077273704612502220135161
3149267999207685605625837242636939222053792080365260847026939793861273604438836830766
8164734539495822108219603207014929994653270346917309546127823781869069725331428314977
4991140789976202143627136239541048931080267447456610339818043575151247074356697868419
5556493750954244363676803142538070823 3,

4721362061963649808863329010234613525807730599160259009967883741918385096173352581810
5231336677923055534666132594041772211881912885394512799835092377732601059788599452596
4356352918107616544158298461436477529796935950078725710677618705985392465973501702267
0275642315020433647342524761924238275541410066296652437630661078222967549760189525938
2259263554535527569833542850838005963854818591738352567759933551953462508281636783296
2300073327840995686403740333517931026 3,

4901462800240748416814014074841827076190073186231138227842097912957955878805324394488
1382079428913414078986519081587055292727934667220189163016586293234469205963267664195
0362141362112901383910428172706086588711061977983758473982770234697478429207874017484
```

```
640860694445336876872412441803830309519377402256773801608451234978451320203460291238946983795733475070849276906136192691974128573534626321644251725135264804943315372217039633339594622712381353920739420199470 3,

420485970579145597958630635373365683138770428963133761653041725352287186214112063193243399009198794940697115014334627159749150070564594917809326213430731801530785419469293337080958121008766495807246629051017536955212049514499180340005448669590071737087784561583796585755051767068376460240691698197991002936873606774141343074347557185123133244906507991775680591075097199618814327703549705991448048413575595104347540154458778200555527823373791889640981452517485410 7,

524862749752293146371487376425943051134397038712954821941693796981018044191813902523454307136152775923455297310420229183779291864745748791083023786201970767392876191394107720917990106409737590833510671216998796968703614409545343857927893583740945893755310835298461875636642261926515526295589225688150688413808034670451962018675243998707231547913062707373351217790138765046542216309147300330941804866893070996946109343838930928529555681028140832811913049393402996 9,

450268484623798536115437423560483887167015867705270599160290283036830775216283287515408987218135740526422070593333132902536552951494813593827911380559702839483572587936266048518474676027032879931259353329085932029475630352681636379821616212631640169017302361808021178880238497414874854113701576932421403924657681536384091552364031299322735138829901806429292834343222064038278344385399530059140059091034110683488685728636107565148462358150648805006535015191878661 ,

453484112624182596851074974433011253719357645968507850868650529127721598464911885662526959326631498190852014903460446717054282757028598783559627799693434744633779767712952142331753318472723319763577285804543416637427380566067189359748867034147472941880401619135051843062941005802021875588206859436303769445203798310577082473057060772111031984537886260745703434924863227606631371329108556798305647067089552901189288549521820753607107063151504851327159668098185307 ,

693532252693819955253847249043757529180324494073823494547591843582136805148466227647256127350410778190683007539432807696698056465273137755794986981751541604145575912570331718107924355720576988204493545005230906033105693432028755478062000534784352638264990268794303011750110045088373921373348481833734839258579645479000424548585936336555233860123720335766312774151565346595485784249448792904040188292802408882242972670662804668689397345518513975596696468318363123 93,

698485168136691724132665829152011148139879620324566495062545610585523848891192898595496554581341746279865107689797681019474530443113784308496947063024856123349076527450913572574975109726895065478134455912406503357880279454439171131741467436488569352478447292667818738642157500636213988618986805702154588288922308406517148587221678802083639421561433645031305963424346113899461348589829576240461675481783419314547546699076853949115857410912538906239326205969606159 1,

652312245560521066216685267046412304641008255275497277851621404823977989959581220590625020743360492343073668835859391198224332970328529845480787899813683059854652628301127724670234965389517976093504678412536278942433021791526475133490313774653515165776970208025720935546643707581729280132057351527379825154329911856872332207538868730085883587106660609079956529803946773881720501869653418632220746434506343490085180086047883798335172360481853965007815045595021699 ,

719413254363295083432127817350409800755190784560072257734440234827616786876995357859887671406367704024677238122954064406134741617051228279482537586743454593130235174717306623960446751614285473609374958027560906050613852195175708585606688316637111592691891702958496518026894008772779789990275042379391572986888580836424672039012717241997440063987107173466301429782677227336252758796833164189919704844725351773049126298708379792690928896517019145432943082569657085 1,

708137525842487067751232432128787750012242832854836219325295271850308759439707344261514746481526501032364937002109243396972728071778971076230354951502983611664258911304271
```

```
695423009335160238263000330011378941227250523182532390858520462473801375711950852185196623408909243650759173702953317340458593296180086045513572795739254820536400341795611975700360763508779386334169188044541210610953812688514320727003703055832388402829147054149821542069118654758440978092954995023285086821140763880680732713134774630698351035597979284186693310580016188513499920233361789635567176147515690925094958082677011319659422843361713526904401914379863383660265588900921137234927934954676282849419802761644394330673026415821404358521144952014204254481242173093088632867330455687429543106186941961544102411745829952413336346125904056130929544227623771245769431308234054154902094426413969393384071589558197509343687178916456762039619181592446495559644 9,

502328508682114076388068073271313477463069835103559797928418669331058001618851349992023336178963556717614751569092509495808267701131965942284336171352690440191437986338366026558890092113723492793495467628284941980276164439433067302641582140435852114495201042454481242173093088632867330455687429543106186941961544102411745829952413336346125904056130929544227623771245769431308234054154902094426413969393384071589558197509343687178916456762039619181592446495559644 9,

385099109380614613946621357676307256032397405617384289899982920397565848770555606321743408300700101396086506173610111444909801037727542670582114217735559372922932344935967525389681465407126753350329756045967097949732046669427853245944760133393974609211856612610989088519675497962626035401516729815675734120153231706980856740092455544373459510039070031865293120630343053546824910219383508420681515780334893557343058853327025318143602405525566185899642616579670433 9,

488231995039863250355020506058037649407480517156548149585037260821037418496444948961969285153948946833678835437881278048625860712787356740225546805518854721202094574102192336548400709041694801486106529120930740414898908172281691726198001799311794376275030136794900208791620428802769648706902393620866220053970680745769660564702211351153786291239520793584390378834841020377097275857110566694357891304425238553735705475787489170575971343761130876456792077287913 1189
    ]

    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.