# Криптографія Комп'ютерний практикум №3 ФБ-05 Чирков Андрій, ФБ-05 Семенов Олексій варіант 10

**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.

#### Хід роботи:

Спочатку була написана функція пошуку випадкового числа, та перевірка цих чисел на простоту через тест Міллера-Рабіна.

Після генеруємо пари р q, р 1 q 1.

Генеруємо пари ключів, для користувачів A і B, де (d,p,q) - секретні ключі, а (n,e) відкриті.

#### Варіанти р які не підходять:

61332624657535893808366832886397851230169719573678652743688833637892789451519

## Варіанти q які не підходять:

 $60478384291040889942378829472892855159989624801198059347575467202480552860252\\ 60368403141870495860511940089658869786487286091952516099743965699550949271860\\ 97856184293896474164376620599208342500776316171579231332570855168721385183217\\ 62031495013776561318862955013022505137895414383316974120618621586427580347592\\ 62094199435034630875778162857917016098084504189739103553168663982943206140075\\ 96415315991012716946307647560032654341635619982276694870977086181425547803958\\ 108414352539993866523188113501618529373665851670487845567736474611732876430244\\ 64033504875905916444000576138931126576044347965712034308956718337381403016478\\ 111514326880082042371785314513954871265844613310356903064602183384388800046250\\ 77026756602259815480308698760803088748503382279014310023680435900410552694689\\ 106355532173969470165223272012264960425538340504834803706129214903072338491205\\ 58662156546625709334229556590131977487618882408303080060349344144743203527330$ 

 $84582463301435280529892074902158073740218387596002630455181241534229170470804\\ 60878190835890823333849689563709781605716437460360407087649092949358206435391\\ 89516846695829628959718861865029111763463603302130790768986079488363533455296\\ 100351601964713134303592051096170641232604940818786435314299408354597488748644\\ 93202214851242945737139482165865300734802721280258473703570950484624655286631\\ 99379141623389588716079534289375959354076632430075899859603779804393500380482\\ 58552758932470142155784004806389205507201966110110352746334196816198023666804\\ 79548551339264391206343136746793099292875682929421170376995858988786241534950\\ 81782695172067528998628351535369082985101692741939652300658384923787452188402\\ 73906325876702552697248364436911509789992949799173640200902514335542967551413$ 

## Варіанти р 1 які не підходять:

 $59060716006034007019951015370277466772437176029690329500337528816627955128558\\99104457433076604013628808265800084348146580655983349101287310332832069459269\\81920281670447853321141182533912402479518893366338492041384294902617513456209\\84677186011403657504686213781422267727980373439762464646390013741875888657132\\99799794131864474073844290665790689519158199413221285662253782502361869365302\\83996565719274554520036246037918810142604504916835585618221207768562834162090\\65268070034626833937087356196169114190281720861353796101504900246956567195751\\1029866347474117891610550554403989184073333171340423781294281098173629861678479\\98544631732154252857766112247291253803988076912640124572306255489146195876086\\82690391965771631576792509597865587023912366797767260516513863841658933146115$ 

#### Варіанти q\_1 які не підходять:

 $58242378551651964633682197124350574387294363505216107005507034195118146783428\\ 60186008865239819235801143417968127042199706908938653866771235823812214233166\\ 76092217080523813895015788781574295611713155085079344098520551318959662507237\\ 74191090622621815847301444113041600309148077215243518730957410745344954013855\\ 97591143698020739476389416370095174408188339110036446003636243812863683608328\\ 77930281641587885641490458833484631706726880900693567625969996751803830595025\\ 100467047158279504501591134130569173162389888922378340114186329468511242740856\\ 77499034770384326092450889641322954815105598687484864262018997257497812077953\\ 71975659046586849588173238131850111145216415584892322233474204108188697723533\\ 85857836197012628782861713310900445589527267356623805588800102345694893750433\\ 78699900176984796022210830053900656661230174501147893946129405344189081412363$ 

1157927319266904955059925921759736725416392173000923788562038239326483005397616902623284295944247004132702765150188645279 00557560850498895420970715935567 6478035089325590447047910733535193965488076301554843961861654772959054291418677170014186573308721535621002144174974337346 28912694098021319248909353115351 : 3264886969863771047466967531490985469090200193797048016605093079805461414131856827857578979332346250863267648826728637609 108979718790252157919309714144335 91652799695418215218181745839946494019442655059428659864183627284145613525127 70680165918045946561822299516144554605093212011605560217601811318568856888113 23966298142872694469895536312305905424984184602990812775426299979092698544307040501392636664407572274027345924386357703 5078159655536023889665707191078835 \_1: 82479716606532948337741506007697928960792968144049495799000959689282269263357240086710051526767928976497668015189264137 7764033440723944041511371184745541 1: 32495809830793743588559253416610507945061281714904009594787225214054832310420837731166030610950569263826166852382144240 2435133810845456002967555826359691 115447999078749380501892850639718821115849685043158542585431054647852126152503 71443175511662086244931447648331059716012181100361281925026527416003429109347 start k: 3194852635298659664100247322181926663852483701652409561388949758186706134047104293389774889083622347317481614912576 terr k. 313463203223623960436247312407362362362466 88223563484586139528983486919483208543 lessage: 5292834498576892026659411350775349747309952295635249755965305617315316199493447410262571019597419769195712946729954 339321064684389656843171649144825421850 he key has been received: 3194852635298059064100247322181926663852483701652409561388949758186706134047104293389774889083622 34731748161491257658023563484586139528983486919483208543 ncrypted message: 514185321221095190816335760970731459609511250140936512252861610733059508713197630239517916489831019869515 38341322527717892459259968255907312283113624028749 Decrypted: message: 52928344985768920266594113507753497473099522956352497559653056173153161994934474102625710195974197691957 12946729954839321064684389656843171649144825421850

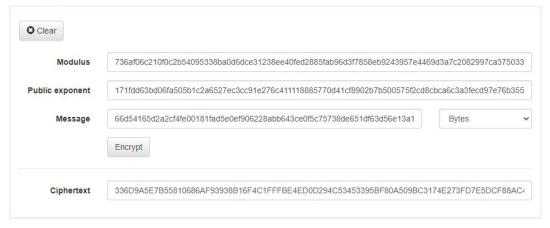
#### Перведемо всі значення в hex для первірки з сайтом

🌄 C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python39\_64\python.exe 0x171fdd63bd06fa505b1c2a6527ec3cc91e276c411118885770d41cf8902b7b500575f2cd8cbca6c3a3fecd97e76b3550e18d5cf51a2521cea20c256 : 0x736af06c210f0c2b54095338ba0d6dce31238ee40fed2885fab96d3f7858eb9243957e4469d3a7c2082997ca375033551c4de2622ede82e5710e65d . sb7bba1f02f680aa6b67aa350f1e67d08860b3973032325f613ef80df0bdfdcb2356f230625486985d3cd526001f309d5479e8af891a6c46b26a2 0xaa6d54eee21134de524a83c223e7dcf646618c1e54fa9f6f15b5a17dc0736939 0xad5eb7140f7f15fec6f683b4800827dbc70f22c6e69a87d461832eea45126511 \_1: 0x68340064f0411f9381ac03ebf56b98905b61d15d16988cee2c6bc360d327448737fbd4c22c9c890b0e8993eea3bfe5c624fd4d5410e01506d9bdc <u>n</u> 1: 0x3128dcc287ecf04c1540c161009d5e307dcf665bcc55487763f71eb906b4d41e7411353f5545dd8b478dd79db5440037869880e885cfb48a7fd3 386570f55af \_1: 0x860765df9fb7ed0d040d04718683f93fe704de7f1874cdae621a23999bb0c6d254c343e783ab5094c10d6a<u>9388b2af036f7103602d8623c406d35</u> 1: 0xd21a41d866bd25990dd6f1044699964956cd0e833b7416bcfb259b43587e3c83 Start k: 0x6d8b0f5d3eeacf1aa4a222dab47ba75d2eb2a1e11241d52fbaabd0f46a6defc4a32afbd1b26d5f8379ce6d90158c5a17115abca5dcf4164c5 b4cd9a99a61ab4 essage: 0x66d54165d2a2cf4fe00181fad5e0ef906228abb643ce0f5c75738de651df63d56e13a1bd42112b66fd<u>7ed8ed2457efec8724ccf8b8c12</u>de78 25050365a3f984 The key has been received: 0x6d8b0f5d3eeacf1aa4a222dab47ba75d2eb2a1e11241d52fbaabd0f46a6defc4a32afbd1b26d5f8379ce6d90158c5a1 7115abca5dcf4164c56b4cd0a99a61ab4 ncrypted message: 0x336d9a5e7b55810686af93938b16f4c1fffbe4ed0d294c53453395bf80a509bc3174e273fd7e5dcf88ac41d899fdf040e7b7525 2d9078d9f407416eaf8587728 Decrypted: message: 0x66d54165d2a2cf4fe00181fad5e0ef906228abb643ce0f5c75738de651df63d56e13a1bd42112b66fd7ed8ed2457efec8724cc f8b8c12de78c25050365a3f984

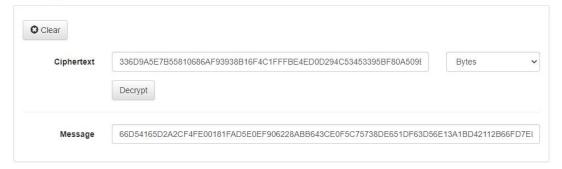
## Get server key



## Encryption



# Decryption



#### Висновок

В лабораторній були розглянуті методи перевірки числа на простоту і генерації ключів для криптосистеми RSA. Було спроектовано систему на основі, що кожен користувач знає лише ті данні, які можуть бути публічними, так само реалізовано методи, на вході лише ті данні, які потрібні для реалізації. Складностями було лише перевірка числа на простоту, але вона вирішується тестом Міллера-Рабіна.