Приложение 2. Демонстрация работы программы

Часть 1. Генератор ключей

In [1]:
```
# Сначала очистим директорию от артифактов предыдущих запусков кода

!rm -f encrypted* decrypted* key.*
!ls -l
```

```
total 148
-rw-r--r-- 1 evgeny evgeny 84294 Apr 23 17:15 demo.ipynb
-rw-r--r-- 1 evgeny evgeny 35117 Apr 23 16:57 image.png
-rw-r--r-- 1 evgeny evgeny  4869 Apr 23 16:57 keygen.py
-rw-r--r-- 1 evgeny evgeny   408 Apr 20 15:36 open.txt
drwxr-xr-x 2 evgeny evgeny  4096 Apr 23 16:59 __pycache__
-rw-r--r-- 1 evgeny evgeny  5160 Apr 23 16:57 rsa.py
drwxr-xr-x 6 evgeny evgeny  4096 Apr 15 15:18 venv
```

In [2]:
```
# Запускаем генерацию ключевой пары
# Скрипт по-умолчанию создаёт пару ключей с названиями "key.pub"
# и "key.secret", или можно напрямую передать скрипту префикс и
# получить пару ключей с другими названиями

# Генератор ключевой пары принимает два парметра p_size и q_size
# Чтобы соблюсти условие значительной величины их разницы -
# задам им разную длину

from keygen import KeyGenerator

KeyGenerator(1024, 3072)

# Проверим создались ли файлы с ключами
!ls -l
```

```
total 156
-rw-r--r-- 1 evgeny evgeny 84294 Apr 23 17:15 demo.ipynb
-rw-r--r-- 1 evgeny evgeny 35117 Apr 23 16:57 image.png
-rw-r--r-- 1 evgeny evgeny  4869 Apr 23 16:57 keygen.py
-rw-r--r-- 1 evgeny evgeny  1541 Apr 23 17:17 key.pub
-rw-r--r-- 1 evgeny evgeny  2053 Apr 23 17:17 key.secret
-rw-r--r-- 1 evgeny evgeny   408 Apr 20 15:36 open.txt
drwxr-xr-x 2 evgeny evgeny  4096 Apr 23 16:59 __pycache__
-rw-r--r-- 1 evgeny evgeny  5160 Apr 23 16:57 rsa.py
drwxr-xr-x 6 evgeny evgeny  4096 Apr 15 15:18 venv
```

In [3]:
```
# Посмотрим содержимое key.pub
# Файл содержит строки в 16-м формате со значением
# e (открытый ключ) и n (модуль) разделенные знаком /

!cat key.pub
```

```
0XB7B2F737E7E8977DA3FEB61416FE89C6F132DBB6FF4C64A9982AF127FBD3FAFC5
06DA369315BC1ADEF328D0BBB65A3EB9BC5D5A4D8F57553B951EC9F3D3CAD58DF42
FE2210F803DB3F023A50A5318639755992B78E50D9BEBD4C8FA33ACA7F136865139
50DB36C24A8D6680FEE15727B4B7B97E60A6D864F4750288A2EF25FBDAF5383C44F
D653B7B0745148795903895385BD3AF82E330178C58E55B495438FAE6F2308FFF27
00AFCF6C045F0D750940DF2626CC0BECE13134B279FCD5B165C629A5730EFBF1E28
9773EA34ACA61B41E1D9E50D603122CCB80B28C9331B5FF20869E3435A69C661804
D2C2F745089AA3A5A3C19FD3C9A6A80B069548BA793C9/0XF23F8E2D7203490DF47
33AC9CA31520AF764E85ADD993BE8EEA6758F46105DE144162E8998455EB9A0ACA3
A62667283AFDA1992CFF39627F727474790597725A968218C42F0B3744311301D1B
7EDCA44A07187B9E9C59833AE8DD0F529F0B0EDE0F293317283D2362C6E71A8D58F
79B5EE0713CEB17202D1B2B954C2318849C7147F889B5D67D9E6D90F748A8B4D8BE
4599F908074EB4FF1F62380B5A22D6FE14E4D05BB8C1BF0F16E96523189D19D07B3
4F68BD10A66ED3A5BE3831E664DDD4F01F27593289918789528 0FE1A393C3B480E0
EEF331A0B49721848F60651D2E811A6361BB0DA8706577673A55AF210F119894134
7BCB1BF0EAFFCCE77C80316AD2B3F67941250CC39DE0BB4AA84290A3D807C461D44
17CC45BA565712F8D73D3CABC35398A7AE860942F011F490C52CF71403DBD0953D1
DEB5D9F183B03AB324A27E11C0316F377F3DB162AFBFEA4AF8BA92FE4A4E29FEF81
236DF3EE2A9D9197273FBF536F631C65866D22E4CF51BFBB8C55383D78B64F88A2A
C24AFBB87E1F4DA75065435574F45F7EB4E4A93E0A2FD55B75075519EEA7B07CD9B
46F7B4A0DFB158CD91D133CF2B87BD1D4C1B0228DDF59BD57CA67E685EB9576861F
AD1984A539FAB3C85C871A1204CF9897F9D765B416A98A526EB1462734116A3928B
F4485891BB2CD6643F143859EE26CD22E388A3684EA5396A75C06FA757A294660C7
```

In [4]:
```
# Посторим файл key.secret
# Файл содержит строки в 16-м формате со значением
# d (закрытый ключ) и n (модуль) разделенные знаком /

!cat key.secret
```

```
0XED844873DF187CFD12C8CC89ED8BF5AD75BB79859F1375E1B981292CD3EBEAFA1
D974172C50D26734542EDA2486D53E3658E374180251E165BCD119C9FF30F8DCB2A
5EA2A8F4C4CC29AAD8A0800B2B7A17AD8E0566D62188DE34892C0FA63C0AC608738
553724A09DCF63055569B7E29E5982D36CA0BF47553C38706615D725FD1F715DA0F
A809CB79F45BE094AD1B5CF36124AD8EACAEE1F82604F4C2E6F106C6C1AF23EED06
DA5B0565C3894B952CB6550A4453A12EAA2AA6E91F2505059E010CB265E0BD9D14A
A4AD6D69D0CE63087386E92872404EEB4850377AE668E2C3021DF63A6762F896CB2
015C34C60615964F873DDBE8F670AC13ABFD971C8B6F7F83FBB4B38A0DF0E21E9F5
98606C9C129A90E370886AD38833608CCB4F2CB948E0593D6E8D005A78B6C2B3A78
A9EFE744B741CE6B4D039C17FC6387B4E3F04C6C18DA5F9E447D71B2CECF845F373
EC0D5C6292E3FEB7B5A01808D08A6E936D5DE2C6DD814C3E710E1995A7833DAF5A0
3B22F7B0FAFE3E88731FC37F4156111C10220FE7CB4239EA82A9F9438ABCCD938F8
021B35D0208DAF973C7D0526FDE0364E1D91E060F4AF08C09150858D7DD8C737C43
53A62E814E84D8AD5D85822317B6925EC67A441D0B182AFC7C160596D026644F82B
C64E0D83ADDFBD5799BFF93C8D189D96BC83321D00D86C520035CF16BB1286BA62D
83B0957797722EB75D729/0XF23F8E2D7203490DF4733AC9CA31520AF764E85ADD9
93BE8EEA6758F46105DE144162E8998455EB9A0ACA3A62667283AFDA1992CFF3962
7F727474790597725A968218C42F0B3744311301D1B7EDCA44A07187B9E9C59833A
E8DD0F529F0B0EDE0F293317283D2362C6E71A8D58F79B5EE0713CEB17202D1B2B9
54C2318849C7147F889B5D67D9E6D90F748A8B4D8BE4599F908074EB4FF1F62380B
5A22D6FE14E4D05BB8C1BF0F16E96523189D19D07B34F68BD10A66ED3A5BE3831E6
64DDD4F01F27593289918789528OFE1A393C3B480E0EEF331A0B49721848F60651D
2E811A6361BB0DA8706577673A55AF210F1198941347BCB1BF0EAFFCCE77C80316A
D2B3F67941250CC39DE0BB4AA84290A3D807C461D4417CC45BA565712F8D73D3CAB
C35398A7AE860942F011F490C52CF71403DBD0953D1DEB5D9F183B03AB324A27E11
C0316F377F3DB162AFBFEA4AF8BA92FE4A4E29FEF81236DF3EE2A9D9197273FBF53
6F631C65866D22E4CF51BFBB8C55383D78B64F88A2AC24AFBB87E1F4DA750654355
74F45F7EB4E4A93E0A2FD55B75075519EEA7B07CD9B46F7B4A0DFB158CD91D133CF
2B87BD1D4C1B0228DDF59BD57CA67E685EB9576861FAD1984A539FAB3C85C871A12
04CF9897F9D765B416A98A526EB1462734116A3928BF4485891BB2CD6643F143859
EE26CD22E388A3684EA5396A75C06FA757A294660C7
```

In [5]:
```
# Создам объект класса RSA для шифрования файлов и
# передам ему ключ для шифрования (открытый)

from rsa import RSA

encryptor = RSA(public_key_path="key.pub")
encryptor
```

Out[5]:
```
<rsa.RSA at 0x7f88152a2e90>
```

In [6]:
```
# Для наглядности вывожу в строчном представлении
# модели и её основные параметры. Видим что объект
# класса обладает только ключами для зашифрования

encryptor.__str__()
```

Out[6]:

```
{'public_key': '0XB7B2F737E7E8977DA3FEB61416FE89C6F132DBB6FF4C64A99
82AF127FBD3FAFC506DA369315BC1ADEF328D0BBB65A3EB9BC5D5A4D8F57553B951
EC9F3D3CAD58DF42FE2210F803DB3F023A50A5318639755992B78E50D9BEBD4C8FA
33ACA7F13686513950DB36C24A8D6680FEE15727B4B7B97E60A6D864F4750288A2E
F25FBDAF5383C44FD653B7B0745148795903895385BD3AF82E330178C58E55B4954
38FAE6F2308FFF2700AFCF6C045F0D750940DF2626CC0BECE13134B279FCD5B165C
629A5730EFBF1E289773EA34ACA61B41E1D9E50D603122CCB80B28C9331B5FF2086
9E3435A69C661804D2C2F745089AA3A5A3C19FD3C9A6A80B069548BA793C9',
 'public_key_int': 2318986108305391351949799348784533712698920595222
353737318040233814439993865491176921452641849960988700330556976740724
245236011653522910038458870500593364264507645305189754701157103852902
025449730766804756099402466620082604752858984239812056345879657149880
804227879791579343442036767756052395208661614987861768978897375125206
060347135903369495889239265268705441880185801175925153698685938106985
853420925565162929132427136200705324067751924206453845904082731225819
191460780072792780746579647628127186609240938213528933609816435822168
683712265598281860349705280953633091674223253816850889820596866455154
543606707885352837635373621810121,
 'public_key_size': 2048,
 'secret_key': None,
 'secret_key_int': None,
 'secret_key_size': None,
 'module': '0XF23F8E2D7203490DF4733AC9CA31520AF764E85ADD993BE8EEA67
58F46105DE144162E8998455EB9A0ACA3A62667283AFDA1992CFF39627F72747479
0597725A968218C42F0B3744311301D1B7EDCA44A07187B9E9C59833AE8DD0F529F
0B0EDE0F293317283D2362C6E71A8D58F79B5EE0713CEB17202D1B2B954C2318849
C7147F889B5D67D9E6D90F748A8B4D8BE4599F908074EB4FF1F62380B5A22D6FE14
E4D05BB8C1BF0F16E96523189D19D07B34F68BD10A66ED3A5BE3831E664DDD4F01F
275932899187895280FE1A393C3B480E0EEF331A0B49721848F60651D2E811A6361
BB0DA8706577673A55AF210F1198941347BCB1BF0EAFFCCE77C80316AD2B3F67941
250CC39DE0BB4AA84290A3D807C461D4417CC45BA565712F8D73D3CABC35398A7AE
860942F011F490C52CF71403DBD0953D1DEB5D9F183B03AB324A27E11C0316F377F
3DB162AFBFEA4AF8BA92FE4A4E29FEF81236DF3EE2A9D9197273FBF536F631C6586
6D22E4CF51BFBB8C55383D78B64F88A2AC24AFBB87E1F4DA75065435574F45F7EB4
E4A93E0A2FD55B75075519EEA7B07CD9B46F7B4A0DFB158CD91D133CF2B87BD1D4C
1B0228DDF59BD57CA67E685EB9576861FAD1984A539FAB3C85C871A1204CF9897F9
D765B416A98A526EB1462734116A3928BF4485891BB2CD6643F143859EE26CD22E3
88A3684EA5396A75C06FA757A294660C7',
 'module_int': 9882866899798064133571318447711131371634408799298986
537991719580458653422015713645654888419677483906593107392949514862668
688863777586363024096549069724558700619827235024668906280979900176453
093495523305805537850979401711275180238725495506633704734434107094983
242179518151826370995646160986393067549850736874006817631790768463
881218706187474726536856306554502313125688522750675775791236131176792
903158439086972588577114764131510873271634160106554190149889973460
579849937455639074206451375476907138588559422024029945152413119519
464518764087227032061756896381726302748528008703117200493136422875
269740616501836583852886128050018603479303825067128318637193251702477
741387538854267550030987923118901808462973898443221630594535223160
505605766845665278615178867280731535104205721571199993603702980152
243505744343238477443433940127709600662007522955704015570735018878
998425976016610990561920923508749121704936161767072736285703567742998
569038045956137790210612642650796485416864034259379649372949179836
540829958291199894081880359732287214037160623148399545547822088704
922507673290190605452285235494937788602478235164260322915471003186
245122897709865230500365130019978978740942754108206219333671037625332
800789425705394282919556539014348579655 1,
 'block_size': 4095,
 'block_size_full': 4096}
```

In [7]:
```
# Создам отдельный объект для расштфрования и
# передам ему закрытый ключ

decryptor = RSA(secret_key_path="key.secret")
decryptor
```

Out[7]:
```
<rsa.RSA at 0x7f87f632f310>
```

In [8]:
```
# Также пристально посмотрим на объект через специальный метод
# Этот объект напротив - содержит лишь ключи для расшифрования
# Таким образом можно ограничить функциональность класса просто
# передав или не передавая ей нужные данные.

decryptor.__str__()
```

Out[8]:

```
{'public_key': None,
 'public_key_int': None,
 'public_key_size': None,
 'secret_key': '0XED844873DF187CFD12C8CC89ED8BF5AD75BB79859F1375E1B
981292CD3EBEAFA1D974172C50D26734542EDA2486D53E3658E374180251E165BCD
119C9FF30F8DCB2A5EA2A8F4C4CC29AAD8A0800B2B7A17AD8E0566D62188DE34892
C0FA63C0AC608738553724A09DCF63055569B7E29E5982D36CA0BF47553C3870661
5D725FD1F715DA0FA809CB79F45BE094AD1B5CF36124AD8EACAEE1F82604F4C2E6F
106C6C1AF23EED06DA5B0565C3894B952CB6550A4453A12EAA2AA6E91F2505059E0
10CB265E0BD9D14AA4AD6D69D0CE63087386E92872404EEB4850377AE668E2C3021
DF63A6762F896CB2015C34C60615964F873DDBE8F670AC13ABFD971C8B6F7F83FBB
4B38A0DF0E21E9F598606C9C129A90E370886AD38833608CCB4F2CB948E0593D6E8
D005A78B6C2B3A78A9EFE744B741CE6B4D039C17FC6387B4E3F04C6C18DA5F9E447
D71B2CECF845F373EC0D5C6292E3FEB7B5A01808D08A6E936D5DE2C6DD814C3E710
E1995A7833DAF5A03B22F7B0FAFE3E88731FC37F4156111C10220FE7CB4239EA82A
9F9438ABCCD938F8021B35D0208DAF973C7D0526FDE0364E1D91E060F4AF08C0915
0858D7DD8C737C4353A62E814E84D8AD5D85822317B6925EC67A441D0B182AFC7C1
60596D026644F82BC64E0D83ADDFBD5799BFF93C8D189D96BC83321D00D86C52003
5CF16BB1286BA62D83B0957797722EB75D729',
 'secret_key_int': 9689837208001500145620398347145656021836148992633938410976366189316021391504649525779295828499113760091171300585566197106411852528810092775650851052213224068002011797023182242418377382862741811636425168307424898282864936913059739982114809602740509857147858948705953597756305900288767209594581669977968685996878906062254405660106051555953280825511302918196654007834054191912100057421858804298303776202161391845647064567864675577329314418476082609703578313070243732019623845216418601275460550321396951711470258582179931884164012356478524260839346958054511771909722216835301686743197210729836722027509610164608573531544754909685942147849882684293596748503194052074954372415929190958458417154143665080263254350837507654882910550518180889935070478375231144186973445099572207673050878081723312736070341627126772005684427803468342548298764499623115388431416125778763627190717382548939540419084121056224900263249120551131393185517716759184132728594765207655387164837577613992105944883017797121874693615454833936009009383947628324798380391639820463903536011699977236770687642855236442055409734830990206182624915586921345166820938384073868778582473545433958435313844193738843457112127077937971244673565067238324872391534305460931972615785572 25,
 'secret_key_size': 4096,
 'module': '0XF23F8E2D7203490DF4733AC9CA31520AF764E85ADD993BE8EEA67
58F46105DE144162E8998455EB9A0ACA3A62667283AFDA1992CFF39627F72747479
0597725A968218C42F0B3744311301D1B7EDCA44A07187B9E9C59833AE8DD0F529F
0B0EDE0F293317283D2362C6E71A8D58F79B5EE0713CEB17202D1B2B954C2318849
C7147F889B5D67D9E6D90F748A8B4D8BE4599F908074EB4FF1F62380B5A22D6FE14
E4D05BB8C1BF0F16E96523189D19D07B34F68BD10A66ED3A5BE3831E664DDD4F01F
275932899187895280FE1A393C3B480E0EEF331A0B49721848F60651D2E811A6361
BB0DA8706577673A55AF210F1198941347BCB1BF0EAFFCCE77C80316AD2B3F67941
250CC39DE0BB4AA84290A3D807C461D4417CC45BA565712F8D73D3CABC35398A7AE
860942F011F490C52CF71403DBD0953D1DEB5D9F183B03AB324A27E11C0316F377F
3DB162AFBFEA4AF8BA92FE4A4E29FEF81236DF3EE2A9D9197273FBF536F631C6586
6D22E4CF51BFBB8C55383D78B64F88A2AC24AFBB87E1F4DA75065435574F45F7EB4
E4A93E0A2FD55B75075519EEA7B07CD9B46F7B4A0DFB158CD91D133CF2B87BD1D4C
1B0228DDF59BD57CA67E685EB9576861FAD1984A539FAB3C85C871A1204CF9897F9
D765B416A98A526EB1462734116A3928BF4485891BB2CD6643F143859EE26CD22E3
88A3684EA5396A75C06FA757A294660C7',
 'module_int': 9882866899798064133571318447711131371634408799298986
5379917195804586534220157136456548884196774839065931073929495148626
6888637775863630240965490697245587006198272350246689062809799001764
5309495523305805537850979401711275180238725495506633704734434107094
9832421795181518263709956461609863930675498507368740068176317907684
6388121870618747472653685630655450231312568852275067577579123613117
```

```
679290315843908697258857711476413151087327163416010655419014988997346057984993745563907420645137547690713858855942202402994515241311951946451876408722703206175689638172630274852800870311720049313642287526974061650183658385288612805001860347930382506712831863719325170247774138753885426755003098792311890180846297389844322163059453522316050560576684566527861517886728073153510420572157119999360370298015224350574434323847744343394012770960066200752295570401557073501887899842597601661099056192092350874912170493616176707273628570356774299856903804595613779021061264265079648541686403425937964937294917983654082995829119989408188035973228721403716062314839954554782208870449225076732901906054522852354949377886024782351642603229154710031862451228977098652305003651300199789787409427541082062193336710376253328007894257053942829195565390143485796551,
 'block_size': 4095,
 'block_size_full': 4096}
```

In [9]:
```
# Хотя можно было все сделать одним объектов
# просто передав ему оба ключа

rsa = RSA(public_key_path="key.pub", secret_key_path="key.secret")
rsa.__str__()
```

Out[9]:
{'public_key': '0XB7B2F737E7E8977DA3FEB61416FE89C6F132DBB6FF4C64A99
82AF127FBD3FAFC506DA369315BC1ADEF328D0BBB65A3EB9BC5D5A4D8F57553B951
EC9F3D3CAD58DF42FE2210F803DB3F023A50A5318639755992B78E50D9BEBD4C8FA
33ACA7F13686513950DB36C24A8D6680FEE15727B4B7B97E60A6D864F4750288A2E
F25FBDAF5383C44FD653B7B0745148795903895385BD3AF82E330178C58E55B4954
38FAE6F2308FFF2700AFCF6C045F0D750940DF2626CC0BECE13134B279FCD5B165C
629A5730EFBF1E289773EA34ACA61B41E1D9E50D603122CCB80B28C9331B5FF2086
9E3435A69C661804D2C2F745089AA3A5A3C19FD3C9A6A80B069548BA793C9',
 'public_key_int': 2318986108305391351949799348784533712698920595222
353737318040233814439993865491176921452641849960988700330556976740724
245236011653522910038458870500593364264507645305189754701157103852902
025449730766804756099402466620082604752858984239812056345879657149880
804227879791579343442036767756052395208661614987861768978897375125206
060347135903369495889239265268705441880185801175925153698685938106985
853420925565162929132427136200705324067751924206453845904082731225819
191460780072792780746579647628127186609240938213528933609816435822168
683712265598281860349705280953633091674223253816850889820596866455154
543606707885352837635373621810121,
 'public_key_size': 2048,
 'secret_key': '0XED844873DF187CFD12C8CC89ED8BF5AD75BB79859F1375E1B
981292CD3EBEAFA1D974172C50D26734542EDA2486D53E3658E374180251E165BCD
119C9FF30F8DCB2A5EA2A8F4C4CC29AAD8A0800B2B7A17AD8E0566D62188DE34892
C0FA63C0AC608738553724A09DCF63055569B7E29E5982D36CA0BF47553C3870661
5D725FD1F715DA0FA809CB79F45BE094AD1B5CF36124AD8EACAEE1F82604F4C2E6F
106C6C1AF23EED06DA5B0565C3894B952CB6550A4453A12EAA2AA6E91F2505059E0
10CB265E0BD9D14AA4AD6D69D0CE63087386E92872404EEB4850377AE668E2C3021
DF63A6762F896CB2015C34C60615964F873DDBE8F670AC13ABFD971C8B6F7F83FBB
4B38A0DF0E21E9F598606C9C129A90E370886AD38833608CCB4F2CB948E0593D6E8
D005A78B6C2B3A78A9EFE744B741CE6B4D039C17FC6387B4E3F04C6C18DA5F9E447
D71B2CECF845F373EC0D5C6292E3FEB7B5A01808D08A6E936D5DE2C6DD814C3E710
E1995A7833DAF5A03B22F7B0FAFE3E88731FC37F4156111C10220FE7CB4239EA82A
9F9438ABCCD938F8021B35D0208DAF973C7D0526FDE0364E1D91E060F4AF08C0915
0858D7DD8C737C4353A62E814E84D8AD5D85822317B6925EC67A441D0B182AFC7C1
60596D026644F82BC64E0D83ADDFBD5799BFF93C8D189D96BC83321D00D86C52003
5CF16BB1286BA62D83B0957797722EB75D729',
 'secret_key_int': 9689837208001500145620398347145656021836148992633
938410976366189316021391504649525779295828499113760091171300585566
197106411852528810092775650851052213224068002011797023182242418377 3
828627418116364251683074248982828649369130597399821148096027405098 5
714785894870595359775630590028876720959458166997796868599687890606 2
254405660106051555953280825511302918196654007834054191912100057421 8
588042983037762021613918456470645678646755773293144184760826097035 7
831307024373201962384521641860127546055032139695171147025858217993 1
884164012356478524260839346958054511771909722216835301686743197210 7
298367220275096101646085735315447549096859421478498826842935967485 0
319405207495437241592919095845841715414366508026325435083750765488 2
910550518180889935070478375231144186973445099572207673050878081723 3
127360703416271267720056844278034683425482987644996231153884314161 2
577876362719071738254893954041908412105622490026324912055113139318 5
517716759184132728594765207655387164837577613992105944883017797121 8
746936154548339360090093839476283247983803916398204639035360116999 7
723677068764285523644205540973483099020618262491558692134516682093 8
384073868778582473545433958435313844193738843457112127077937971244 6
735650672383248723915343054609319726157855722 5,
 'secret_key_size': 4096,
 'module': '0XF23F8E2D7203490DF4733AC9CA31520AF764E85ADD993BE8EEA67
58F46105DE144162E8998455EB9A0ACA3A62667283AFDA1992CFF39627F72747479
0597725A968218C42F0B3744311301D1B7EDCA44A07187B9E9C59833AE8DD0F529F
0B0EDE0F293317283D2362C6E71A8D58F79B5EE0713CEB17202D1B2B954C2318849
C7147F889B5D67D9E6D90F748A8B4D8BE4599F908074EB4FF1F62380B5A22D6FE14
E4D05BB8C1BF0F16E96523189D19D07B34F68BD10A66ED3A5BE3831E664DDD4F01F

```
27593289918789528OFE1A393C3B480E0EEF331A0B49721848F60651D2E811A6361
BB0DA8706577673A55AF210F1198941347BCB1BF0EAFFCCE77C80316AD2B3F67941
250CC39DE0BB4AA84290A3D807C461D4417CC45BA565712F8D73D3CABC35398A7AE
860942F011F490C52CF71403DBD0953D1DEB5D9F183B03AB324A27E11C0316F377F
3DB162AFBFEA4AF8BA92FE4A4E29FEF81236DF3EE2A9D9197273FBF536F631C6586
6D22E4CF51BFBB8C55383D78B64F88A2AC24AFBB87E1F4DA75065435574F45F7EB4
E4A93E0A2FD55B75075519EEA7B07CD9B46F7B4A0DFB158CD91D133CF2B87BD1D4C
1B0228DDF59BD57CA67E685EB9576861FAD1984A539FAB3C85C871A1204CF9897F9
D765B416A98A526EB1462734116A3928BF4485891BB2CD6643F143859EE26CD22E3
88A3684EA5396A75C06FA757A294660C7',
 'module_int': 9882866899798064133571318447711131371634408799298986
5379917195804586534220157136456548884196774839065931073929495148626
6888637775863630240965490697245587006198272350246689062809799001764
5309495523305805537850979401711275180238725495506633704734434107094
9832421795181518263709956461609863930675498507368740068176317907684
6388121870618747472653685630655450231312568852275067577579123613117
6792903158439086972588577114764131510873271634160106554190149889973
4605798499374556390742064513754769071385885594220240299451524131195
1946451876408722703206175689638172630274852800870311720049313642287
5269740616501836583852886128050018603479303825067128318637193251702
4777413875388542675500309879231189018084629738984432216305945352231
6050560576684566527861517886728073153510420572157119999360370298015
2243505744343238477443433940127709600662007522955704015570735018878
9984259760166109905619209235087491217049361617670727362857035677429
9856903804595613779021061264265079648541686403425937964937294917983
6540829958291199894081880359732287214037160623148399545547822088704
4922507673290190605452285235494937788602478235164260322915471003186
2451228977098652305003651300199789787409427541082062193336710376253
3280078942570539428291955653901434857965 51,
 'block_size': 4095,
 'block_size_full': 4096}
```

In [10]:
```
# Проверим правильность работы ключей у объектов encrypted
# и decrypted. Сгенерируем случайное число и зашифруем а
# затем расшифруем их

import random

_int = random.randrange(2, 100)

encr = pow(_int, encryptor.public_key_int, encryptor.module_int)
decr = pow(encr, decryptor.secret_key_int, decryptor.module_int)

bool(decr == _int)
```

Out[10]: True

In [11]:
```
# Проделаем то же самое с объектом rsa чтобы подтвердить
# корректность суждений

_int = random.randrange(2, 100)

encr = pow(_int, rsa.public_key_int, rsa.module_int)
decr = pow(encr, rsa.secret_key_int, rsa.module_int)

bool(decr == _int)
```

Out[11]: True

Часть 2. Зашифрование и расширование

In [12]:
```
# Для демонстрации зашифрования и расшифрования мною были
# подготовлены два файла с тескстом open.txt и изображением
# image.png

# Передам методу encrypt относительный путь к файлу для
# зашифрования и название файлы куда дб записан зашифрованый
# файл encrypted.txt

rsa.encrypt("open.txt", "encrypted.txt")
```

In [13]:
```
# Попробуем прочитать зашифрованый файл

!cat encrypted.txt
```

```
□□□□□       W□k↯⊛&S□▷0□^⍉□T□◷[ᘯ□□e3W⁖km□ZV□=□b1□L□
□^KY□>□q□⌕y~□□□⍝□□□□□□□|h□□ᛉ□{□□c1□□v:□~5□M
C;□ȩ
□□♪□}rl□zO□/¨'∝◂□□*Q□。$□▷R□p`□□ьⵁEO=□Iн□B□.)□l□□La
□"□□□d□n□Su□□A □□□►<□◂□□□□□%⊰i□♂E⊰□ᓯ□D⌀□"ŏ>P
□>G"□[牉♪□ᘘD◷ᘘ□□~□□o□4□}⌐陬e□E□ɯ%□e⊴□~□□□ᛉF□□□
□□□□=☎□□□□L□⌐□□□□ï□w⁘gLY♀♫□□□⊛□tB♪⊵□□⊵¤□t□r
=☎□ □□⊰□\♫□□□□PBH□□r□¤□E  Z̈C□
□♪ɣ□f□P□□□□□B¨□□♪□0.P□□<□◷t_□□□\□Kqw□B□□G□I`
□ᘘ□  }^{x□□;□k□,□□w□□□&□Z□□ĵ□o□!ى□□)n□□□~v1。N
□□□□□□□H∝⁓!1Y□◷e□□□ĬZQ□□TZ*□∝^□H□◂□S[*Kzu□x□
w⊛]□-+□
```

In [14]:
```
# Передам методу decrypt относительный путь к файлу для
# расшифрования и название файлы куда дб записан расшифрованый
# файл decrypted.txt

rsa.decrypt("encrypted.txt", "decrypted.txt")
```

In [15]:
```
!cat decrypted.txt
```

```
Прощай немытая Россия,
Страна рабов, страна господ,
И вы, мундиры голубые,
И ты, им преданный народ.

Быть может, за стеной Кавказа
Сокроюсь от твоих пашей,
От их всевидящего глаза,
От их всеслышащих ушей.

Михаил Лермонтов, 1841г.
```

In [16]:
```
# Установлю библиотеку для просмотра изображений

!pip3 install pillow
```

```
Defaulting to user installation because normal site-packages is not
writeable
Requirement already satisfied: pillow in /usr/lib/python3/dist-pack
ages (9.4.0)
```

In [17]:
```
# Зашифрую изображение и сохраню в файл encrypted.png

rsa.encrypt("image.png", "encrypted.png")
```

In [18]:
```
# Попробую открыть файл

from PIL import Image

try:
    Image.open("encrypted.png")
except:
    print("Невозможно прочитать файл!")
```

```
Невозможно прочитать файл!
```

In [19]:
```
# Расшифрую изображение и сохраню в файл decrypted.png

rsa.decrypt("encrypted.png", "decrypted.png")
```

In [20]:
```
# Попробую открыть файл

Image.open("decrypted.png")
```

Out[20]:

Спасибо за внимание и да пребудет с вами сила!