**Практическая работа № 1**

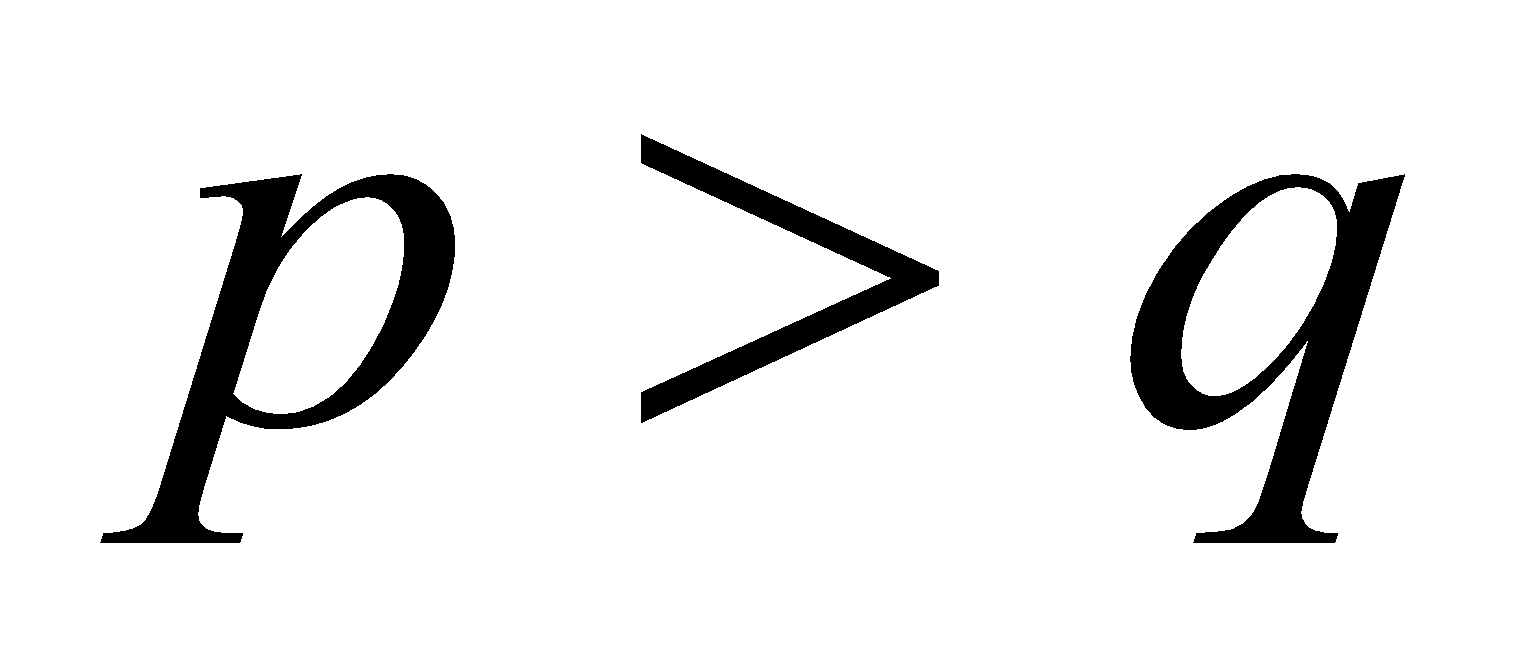
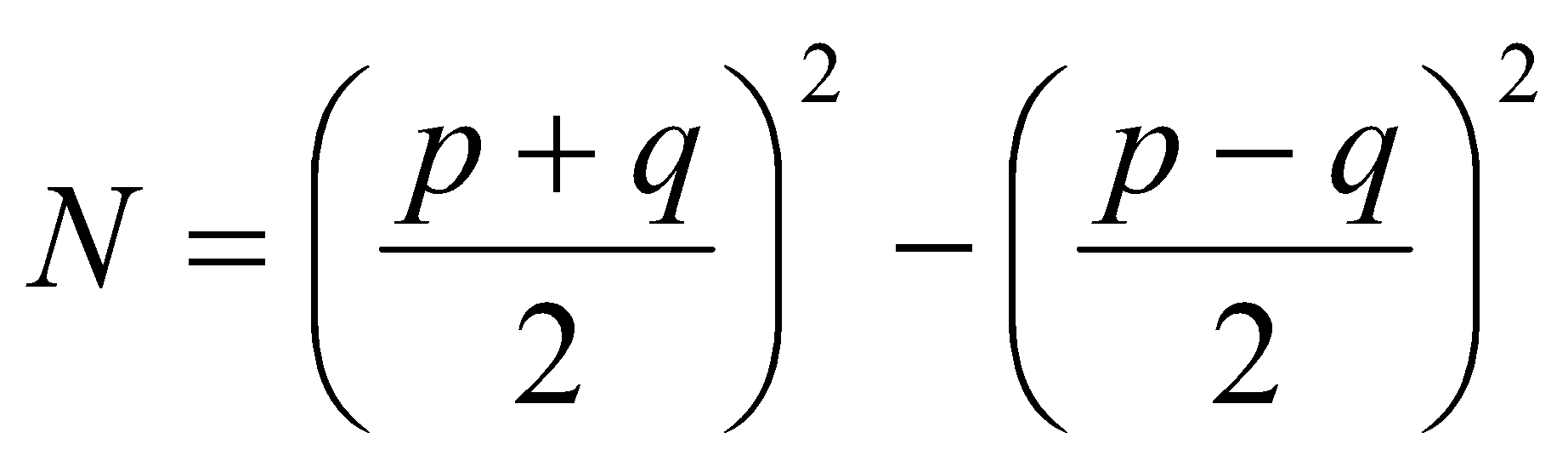
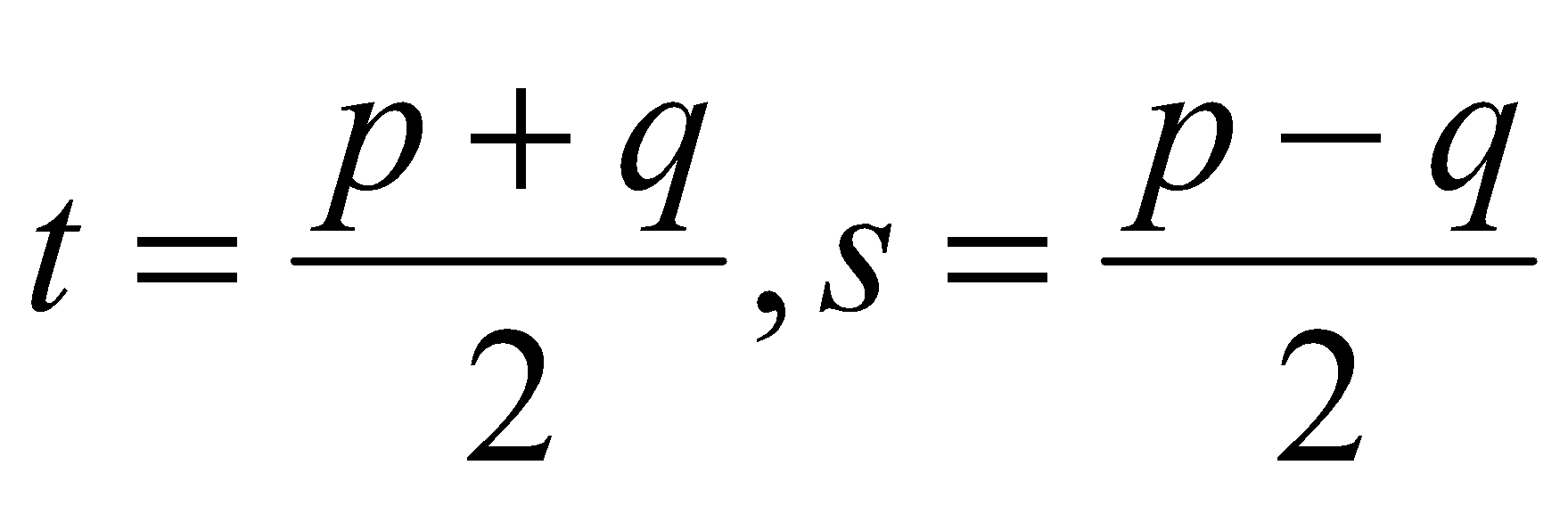
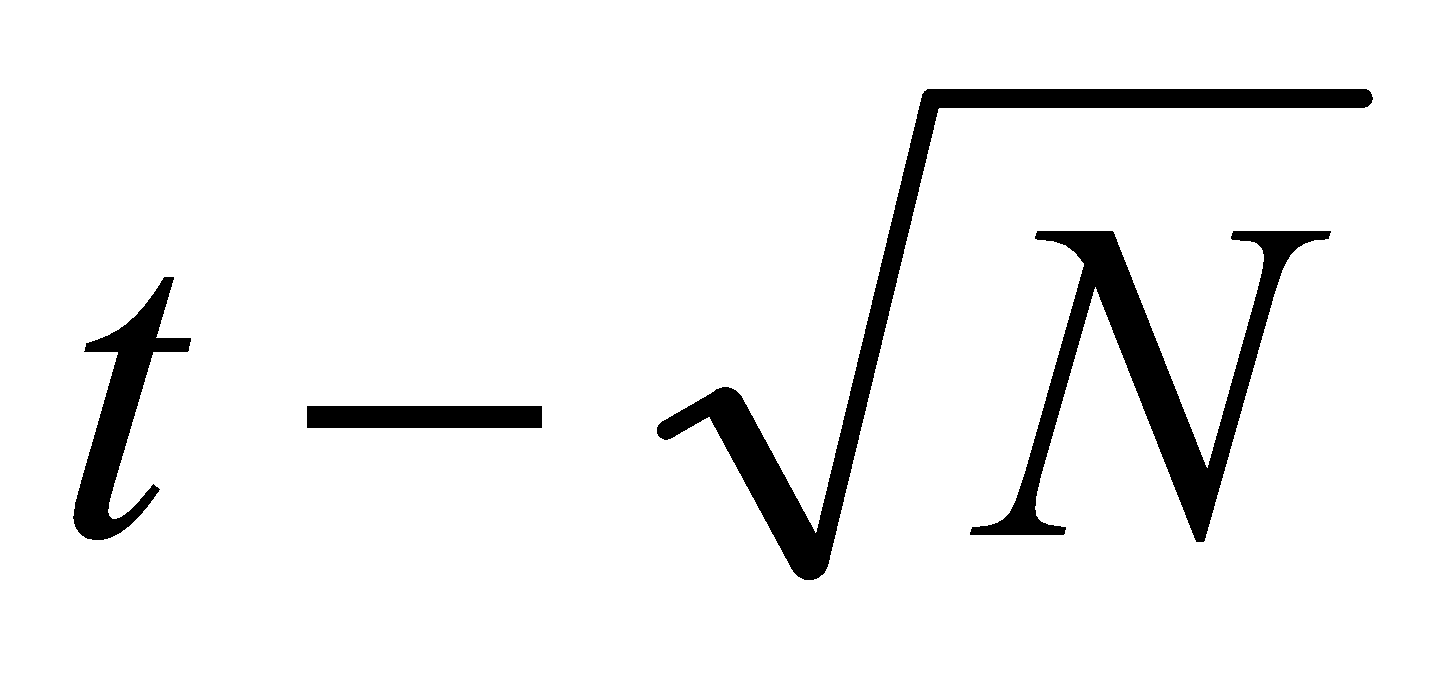
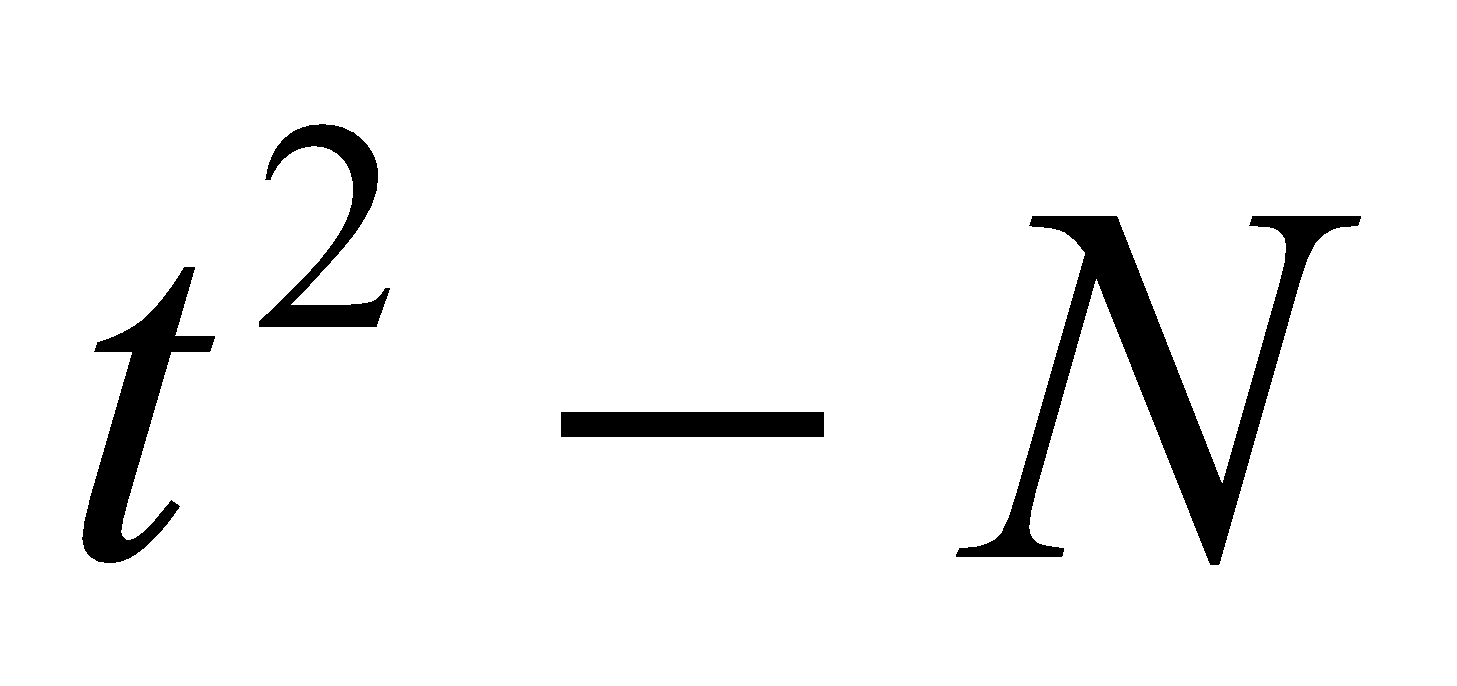
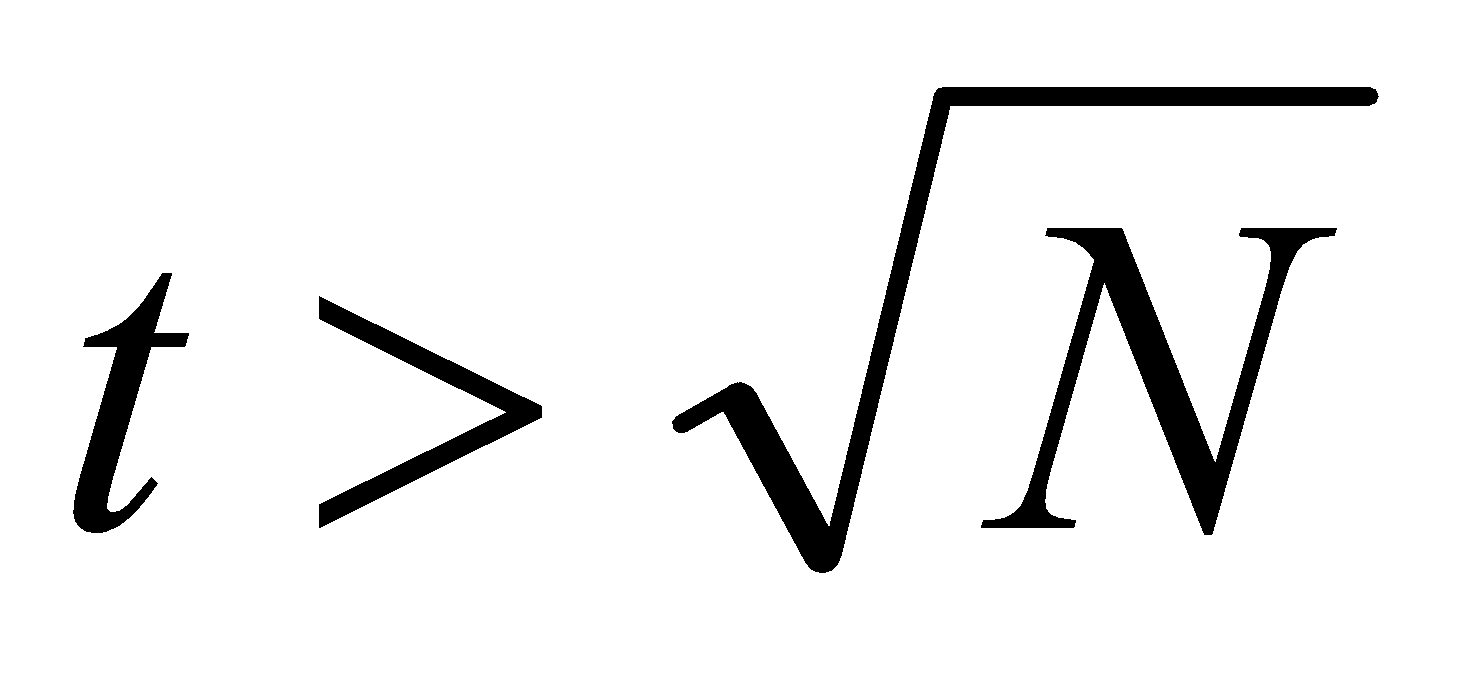
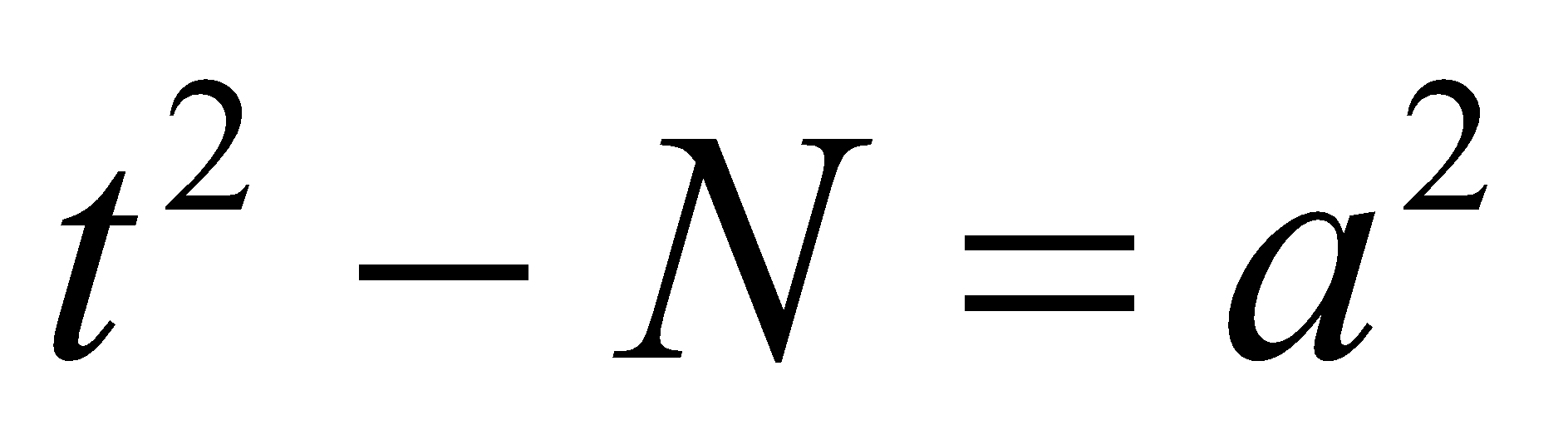
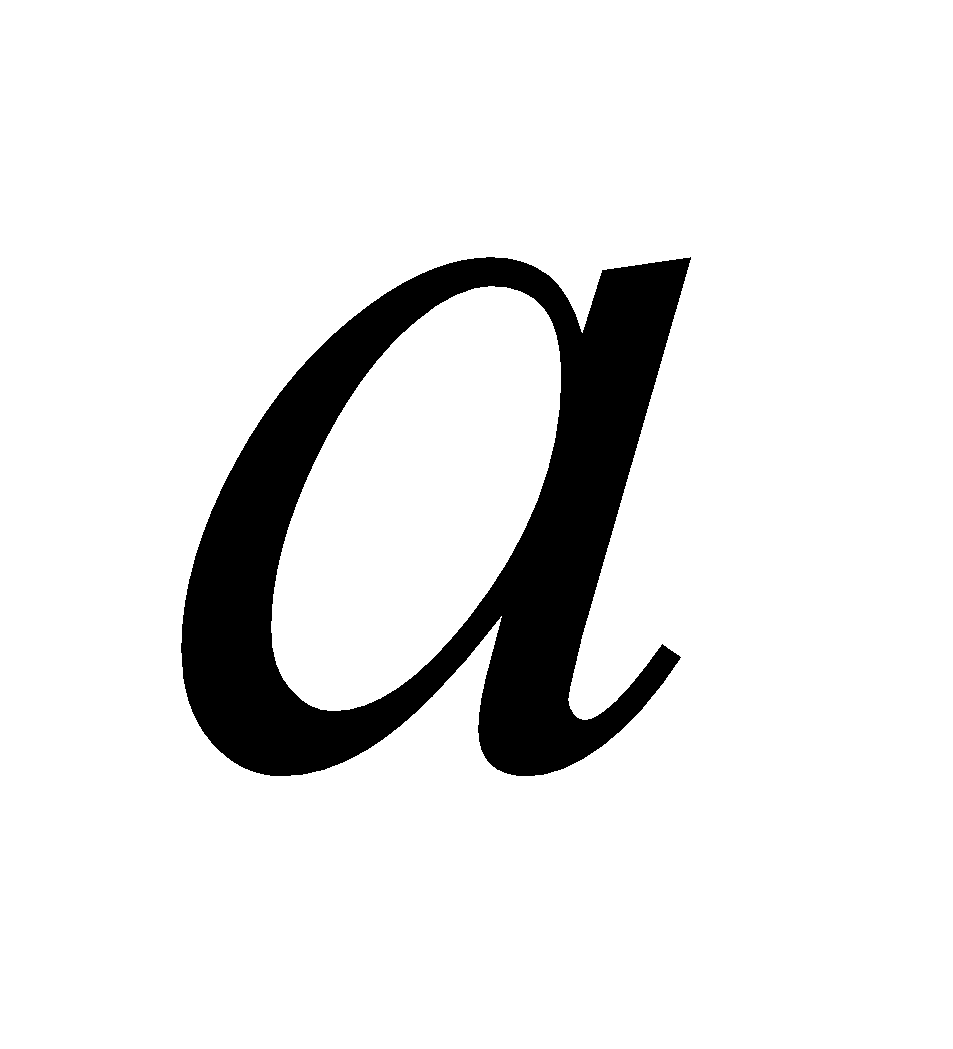
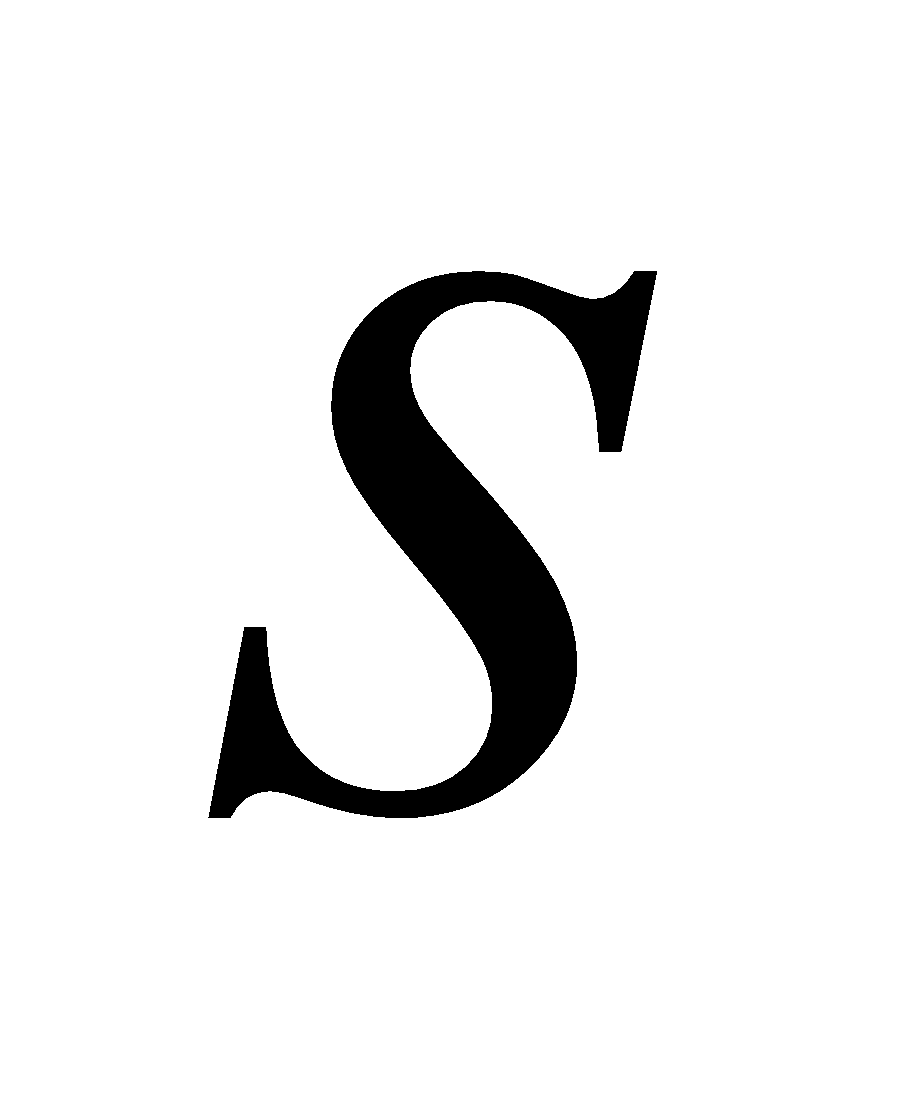
**АТАКА НА АЛГОРИТМ ШИФРОВАНИЯ RSA ПОСРЕДСТВОМ МЕТОДА ФЕРМА**

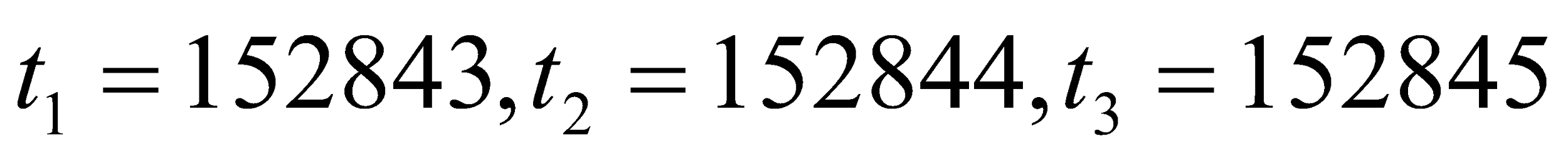
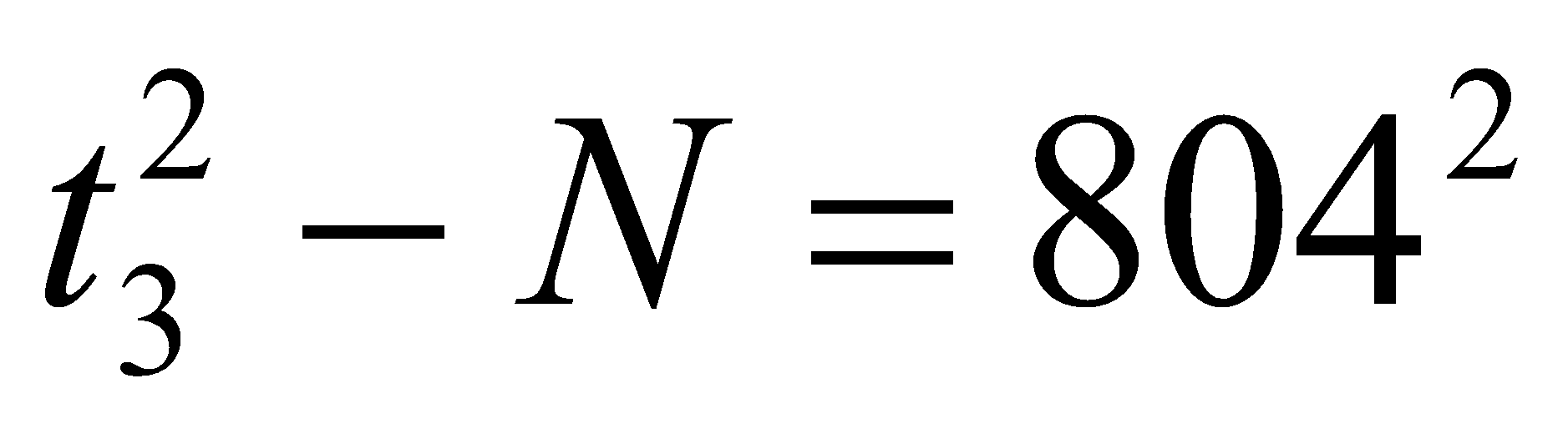
***Цель работы****:* изучить атаку на алгоритм шифрования RSA посредством метода Ферма для случая неудачного выбора параметров.

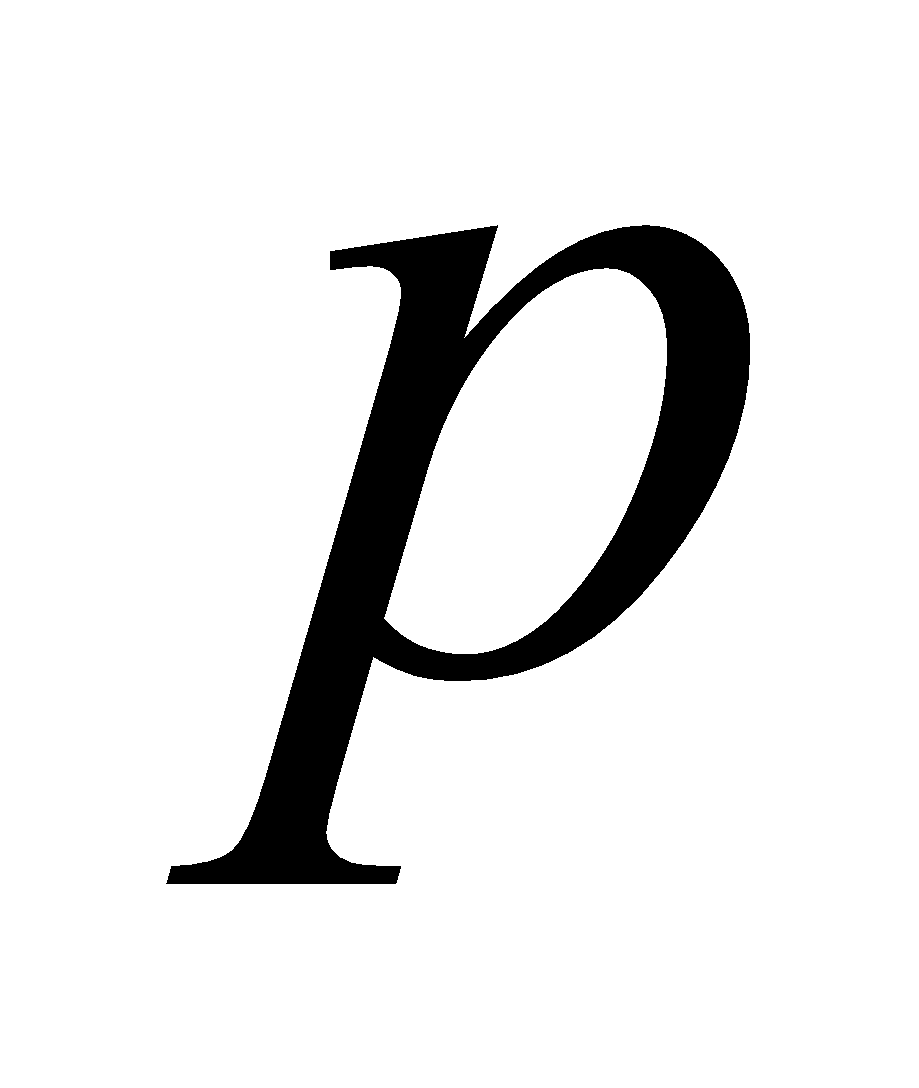
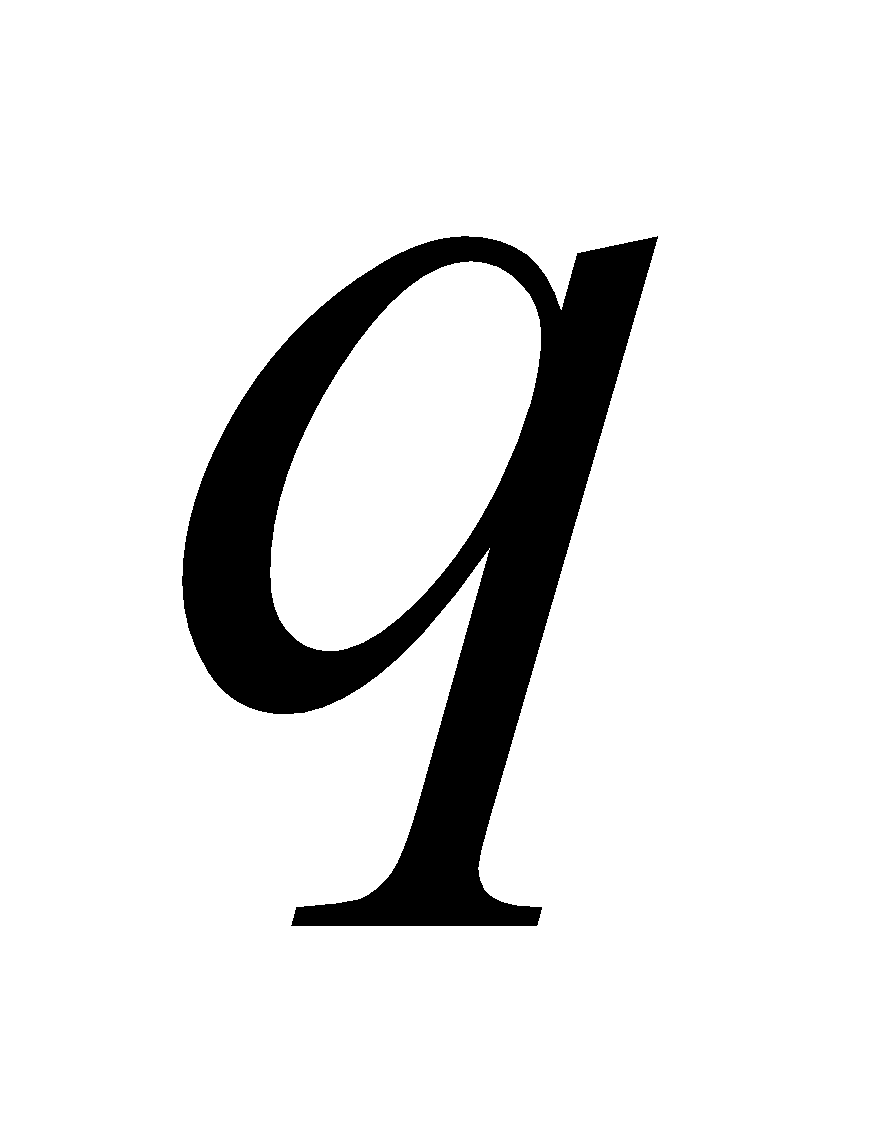
***Взлом алгоритма RSA при неудачном выборе параметров криптосистемы***

Обеспечение безопасности RSA зависит от реализации этого метода. Неудачный выбор параметров позволяет найти эквивалентные ключи или факторизовать модуль. Рассмотрим ряд примеров.

*Пример 1.* Пусть *N* = 2047, *e* = 179, *d* = 411. Так как 2047 = 23×89, а φ(23) = 22, φ(89) =88 имеют наименьшее общее кратное 88, то любой обратный к 179 по модулю 88, например 59, будет действовать как *d*.

*Пример 2*. Число 23360947609 является очень плохим выбором для *N* из-за того, что два его простых делителя слишком близки к друг другу. Пусть , тогда . Пусть , т.к. последняя величина небольшая, то и  также является небольшим числом и  является полным квадратом. Переберем все числа  и проверим на выполнение условия , где  и есть :

 и 

Далее нахождение  и  не представляет большого труда.

***Ход работы:***

1. исходные данные для своего варианта взять из табл. 1;
2. используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:
   * множители модуля (*p* и *q*);
   * значение функции Эйлера для данного модуля φ(*N*) ;
   * обратное значение экспоненты по модулю φ(*N*) ;
3. дешифровать зашифрованный текст, исходный текст должен быть фразой на русском языке;
4. результаты и промежуточные вычисления оформить в виде отчета.

**Варианты заданий к выполнению практической работы № 1**

Таблица 1.

| Вариант | Модуль (*N*) | Экспонента (*е*) | Блоки зашифрованного текста |
| --- | --- | --- | --- |
| 13 | 72903890242273  t = 8538383  s = 9696  phiN = 72903873165508  d = 16406932632835 | 3261683  p = 8528687  q = 8548079 | 37429454018574 4059818986  65632293727338 3894472160  71955235122455 552792288  71474662312159 3992055790  18537435780920 4042452462  58372142077460 3961582576  68330829196451 4007849445  60882917270796 539828463  24142764117328 4042194914  31238010810556 3959416306  66143215653810 4060029165  30769266886306 3760217951 |
| 19 | 59046883376179  t = 7684202  s = 8775  phiN = 59046868007776  d = 31944145322807 | 4044583  p = 7675427  q = 7692977 | 32279109612093 4092653282  17838629182964 3991219744  4165776716262 3487953125  13093284635895 4159238635  20048651313008 3907789039  54626454832531 4041795565  12801053743903 3773491232  54675332003643 3991272948  4544911979279 4108708594  31928373564570 3907186158  798945495513 3824034024  19569174668782 4059033323 |
| 23 | 48992988576733  t = 6999503  s = 7326  phiN = 48992974577728  d = 25037979834125 | 4545733  p = 6992177  q = 7006829 | 12530303611339 4008702696  47274247086952 3974163452  20068556933394 3992710176  41300245344157 1297372448  27564916776233 3990888691  45997492729411 4042187501  11416336760074 3844097100  17516700753417 1126965484  10586755223028 3773556205  5642378694993 4243253481  17949047899806 539551979  13276902592875 3894435679 |
| 29 | 33644210466973  t = 5800367  s = 6846  phiN = 33644198866240  d = 18224590060541 | 5285461  p = 5793521  q = 5807213 | 2887763929737 4008898544  14268468183889 3772967648  17106478222082 552263908  11308338337725 4042187296  22932870001788 3808161774  22780920502986 3958243301  3159009422412 4075945760  22191880208231 4059095271  24883589317156 4079022062  20042326937734 4058768672  21464252061935 3908378719  6743660373779 1600085855 |

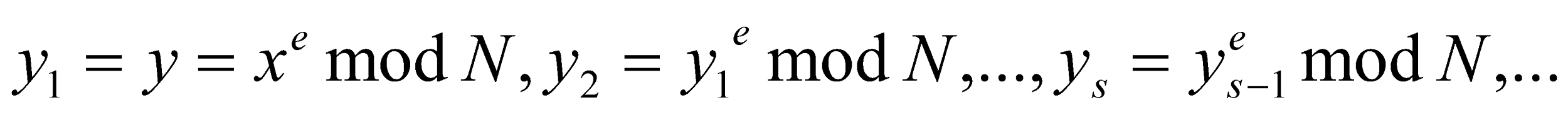
**Практическая работа № 2**

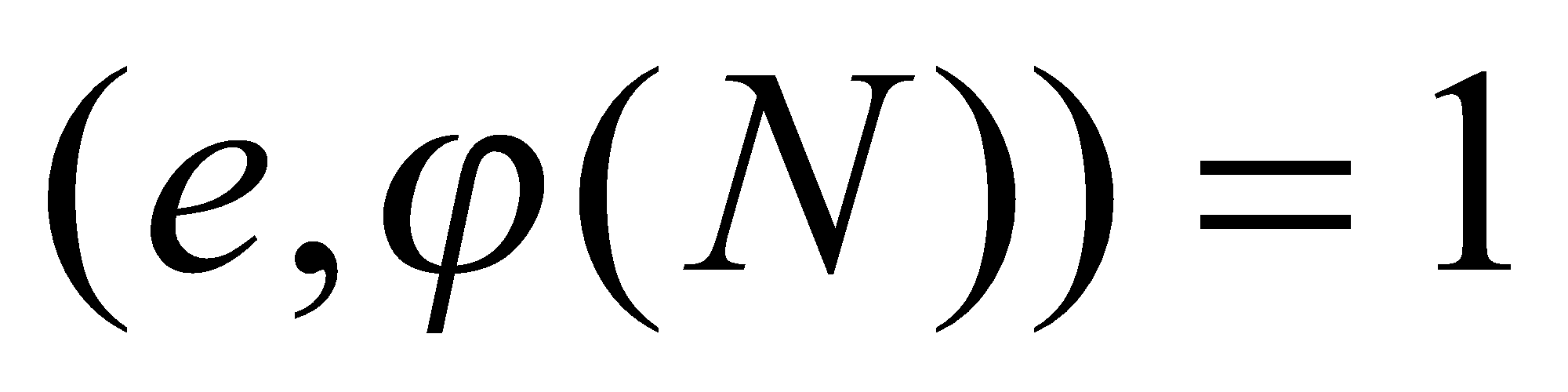
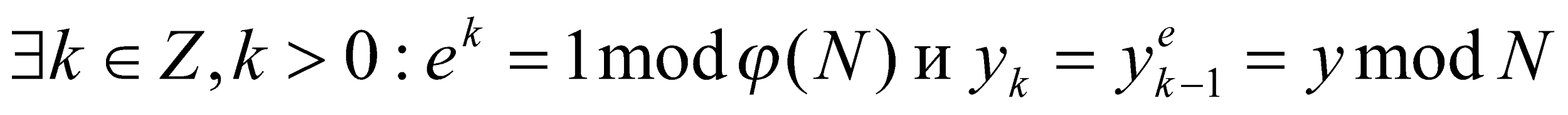
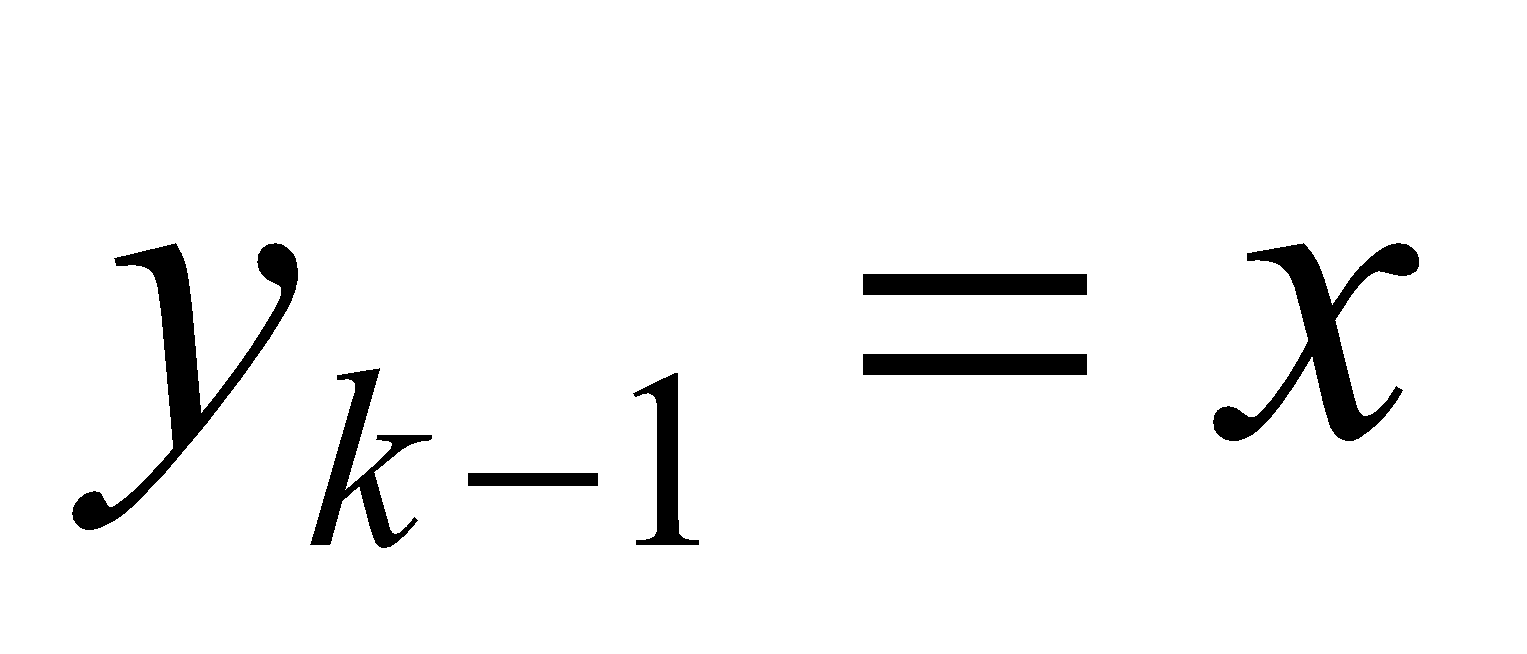
**АТАКА НА АЛГОРИТМ ШИФРОВАНИЯ RSA МЕТОДОМ ПОВТОРНОГО ШИФРОВАНИЯ**

***Цель работы****:* изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

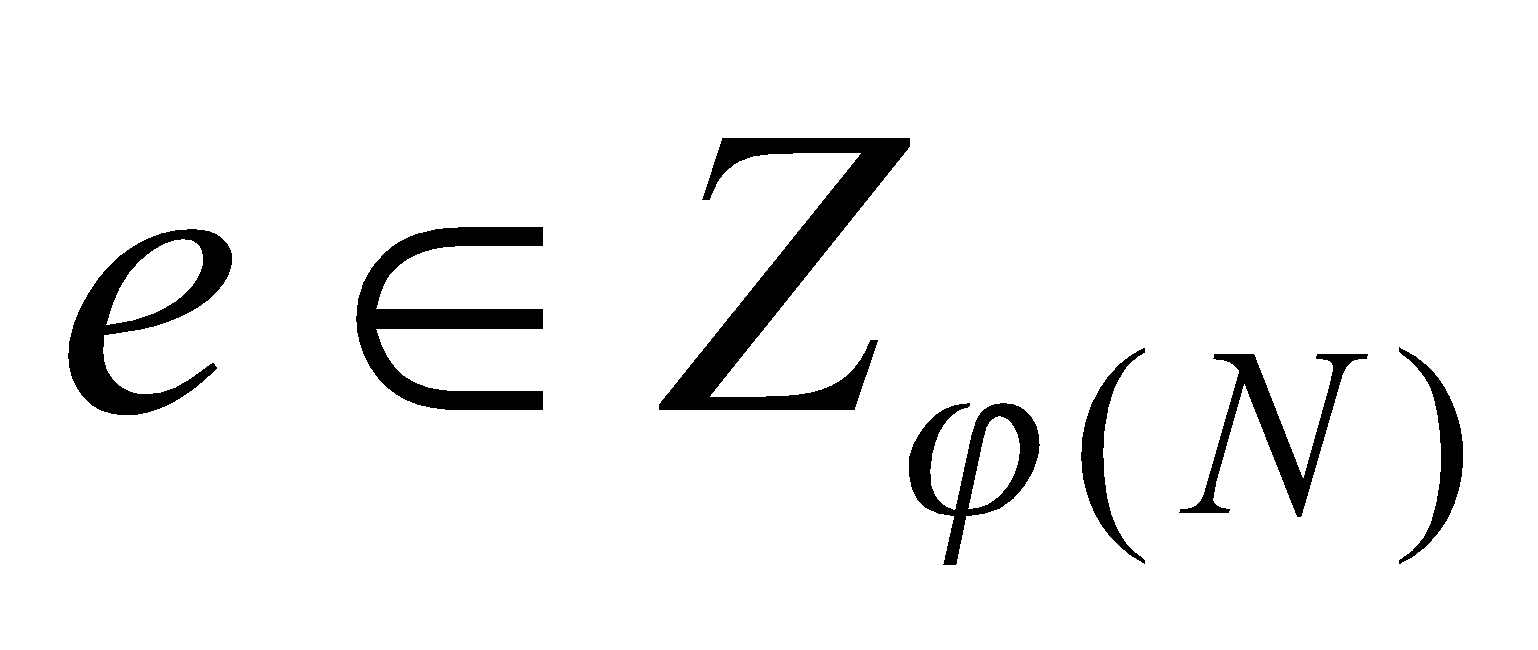
**Атака повторным шифрованием**

Рассмотрим последовательность



Так как , то , следовательно .

***Ход работы:***

1. по исходным данным варианта используя идею перешифрования определить порядок числа ;
2. используя значение порядка экспоненты, получить исходный текст методом перешифрования;
3. результаты и промежуточные вычисления оформить в виде отчета.

**Варианты заданий к выполнению практической работы № 2**

Таблица 2

| Вариант | Модуль (*N*) | Экспонента (*е*) | Блоки зашифрованного текста |
| --- | --- | --- | --- |
| 13 | 915012974539  k = 4919 | 1001953 | 763770087861 4092719856  432343847598 3773687277  764682728575 3909034223  206635140312 4042187243  627210520886 3857513262  794063631890 549777121  309297959146 3772967909  68118108284 3991463200  116045398315 3974687472  912085643674 4008702190  257483784869 4142264817  167814127445 4008763436  55188158350 550422483 |
| 19 | 762930465497  k = 68639 | 369197 | 272601390768 4075155954  146191862405 3908103906  56417639739 3773688063  25010208392 552083682  569176485965 4226805483  292815488501 3991268840  152909580675 4280346592  634319609453 4025544433  578700740159 4007796776  648142948177 3990888701  39319966771 4075692065  517127377434 4059033329  490584971826 4007783931 |
| 23 | 888532740131  k = 78539 | 508097 | 251133768996 3907908325  359801014616 3992053986  557356431645 3991859698  75854873865 4230016760  768478933532 3907120874  624174758081 740352032  306027834198 4074826470  586384787006 3844140783  155294489444 4041598181  358096762086 3957912316  197284968232 552530413  498688500894 4007849467  467532994504 3844104031 |
| 29 | 414634315817  k = 68819 | 1039187 | 200343263939 1382641255  13939901815 740352032  329718769183 4074826470  169659670872 3844141038  49667978685 3841062885  11286581382 4062243552  92461615100 3840995042  173590557244 539550240  62542045222 4075744288  310782145259 4159238635  348390168011 3844104818  308011216304 1868653667  154928746700 1634956329 |

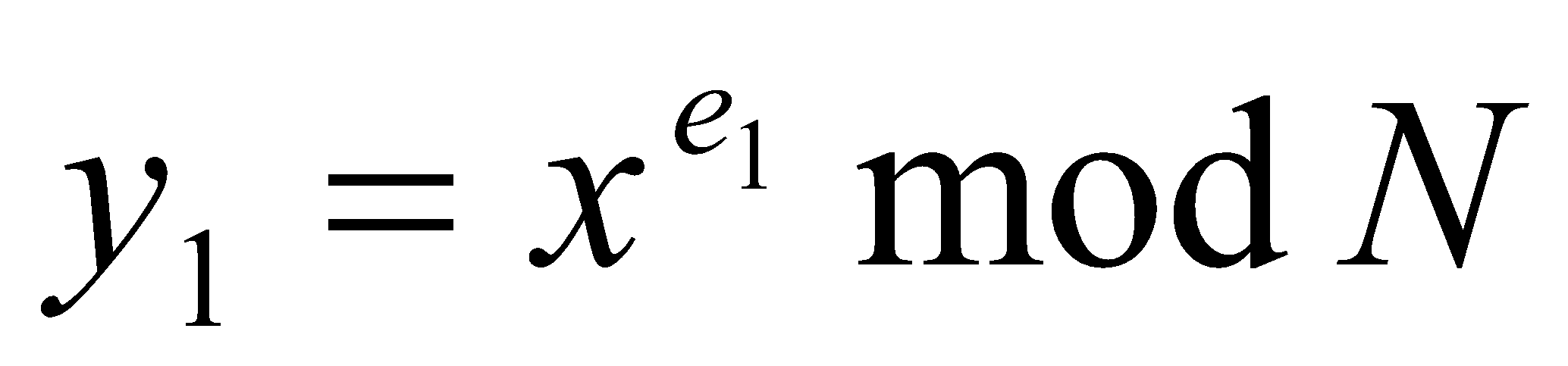
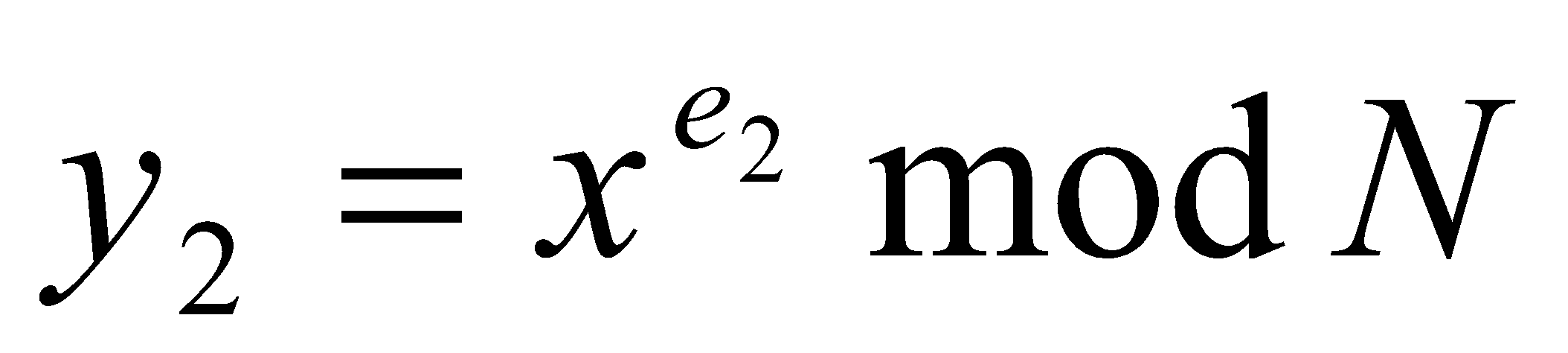
**Практическая работа № 3**

**АТАКА НА АЛГОРИТМ ШИФРОВАНИЯ RSA МЕТОДОМ БЕСКЛЮЧЕВОГО ЧТЕНИЯ.**

***Цель работы***: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

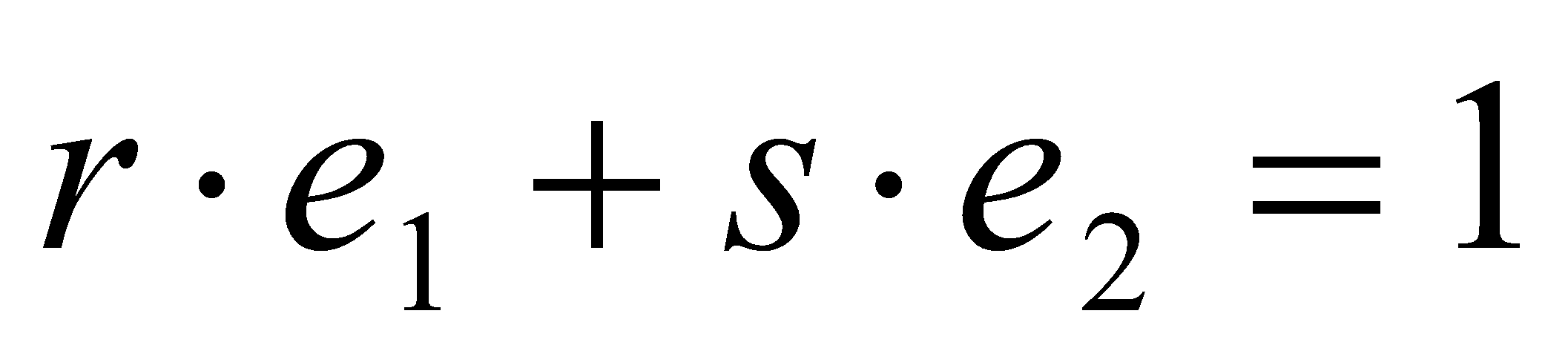
**Метод бесключевого чтение**

Пусть два пользователя выбрали одинаковый модуль *N* и разные экспоненты ***e*1** и ***e*2**. Третий пользователь посылает им некое циркулярное сообщение ***x***, то криптоаналитик может получить в свое распоряжение два шифрованных текста

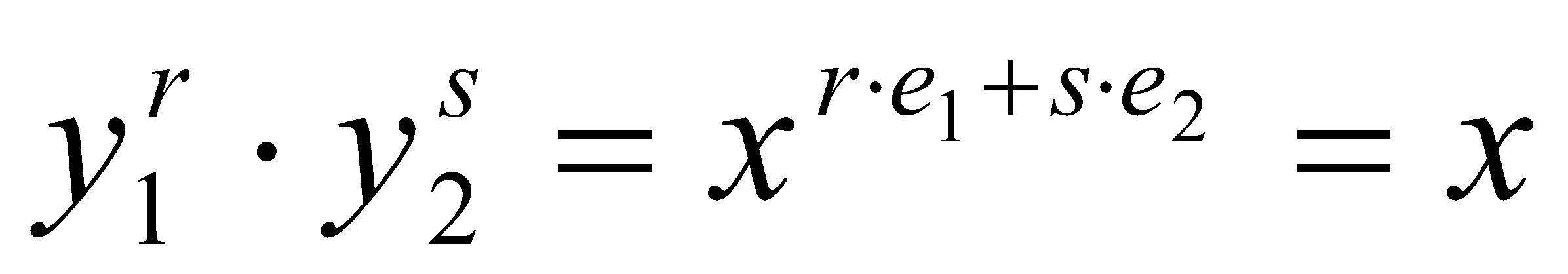
 и 

В этом случае криптоаналитик может получить исходное открытое сообщение, используя расширенный алгоритм Евклида, выполнив следующую последовательность действий:

* находим *r*, *s* такие, что



* получаем открытое сообщение

.

***Ход работы:***

1. по исходным данных варианта задания определить значения *r* и *s*
2. используя полученные значения *r* и *s*, записать исходный текст;
3. результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета.

**Варианты заданий к выполнению практической работы № 3**

Таблица 3

| Вариант | Модуль(*N)* | Экспоненты | | Блоки зашифрованного текста | | |
| --- | --- | --- | --- | --- | --- | --- |
| e1 | e2 | y1 | y2 |  |
| 13 | 518587807081  r = 559972  s = -135703 | 293177 | 1209781 | 373852443734  447989059513  140756140384  207791711792  252160015422  151272799305  431450717984  252882800366  112417596471  301753741810  480461056512  334158277030  368394150653 | 22286870422  343015689591  281801228231  360270382562  264253306719  128520421967  399665129411  448878989738  70913527757  295285211952  247990966487  202711954425  201121363025 | 3488671776  4058965988  3773688040  552726245  3840470501  3991469856  4059229936  4008573728  4007783653  3991462624  4277334527  552461809  3941474336 |
| 19 | 500984306287  r = 82649  s = -145100 | 470149 | 267797 | 274230487503  6821302647  172152295595  454539302130  462305524774  73589652382  274794725040  295185494003  159348742119  62021560582  311827395163  159638616315 | 176943898057  272954693703  141643708385  238296127866  270971764501  389314459147  476866404163  295344931481  288885538254  144738759088  52793710114  416204845784 | 4074826470  3844140270  3873829408  4092256487  3774020640  4058378466  3857773344  3974163185  3907838187  4243454953  552657127  3974492192 |
| 23 | 303958823183  r = -439603  s = 377478 | 1173551 | 1366693 | 300865234944  280167078723  44778324729  15647443106  72500796041  127042219796  220297476381  159193146152  281783946206  83397684706  218587175059  32628200905  87293077359 | 158205869566  47430389231  235868270647  60933642983  230961885063  189840956692  155026770625  118061171422  64695094087  90093203015  140628953794  156685525752  96578125026 | 4159237600  552067306  3959355360  3857904127  551690482  4008455200  4159893024  3990940648  4159235360  3974489834  3773100270  3807306734  538976288 |
| 29 | 1176879950087  r = 127008  s = -185723 | 550169 | 376237 | 236505725833  12096288569  1062670335800  541231133081  529745761698  79574674510  518908160088  195753762481  284194617926  861518052504  844805726716  575330762793  319168661888  377123370130 | 169179266140  617962027334  332483986069  1065692323879  420409290920  733896529297  201622748685  457529162746  1037225648947  732504268577  1172056967964  1002467039854  850197148213  279510203667 | 808335670  552397553  551873535  540094512  550298088  4063228192  686960160  3845005537  3857179374  3890409696  4075679264  4075155711  3857904127  538976288 |