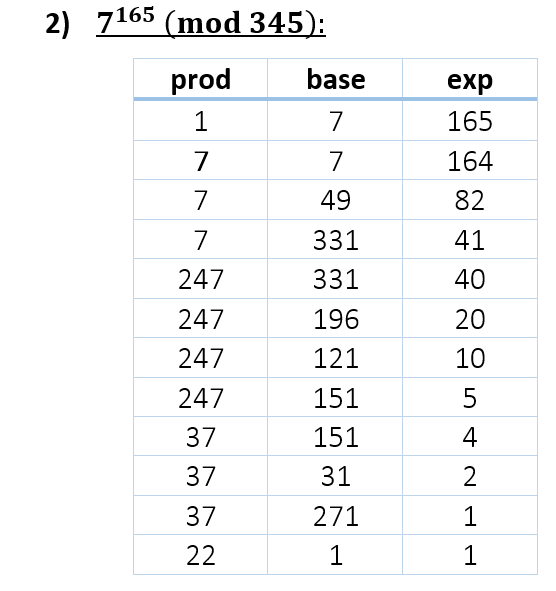
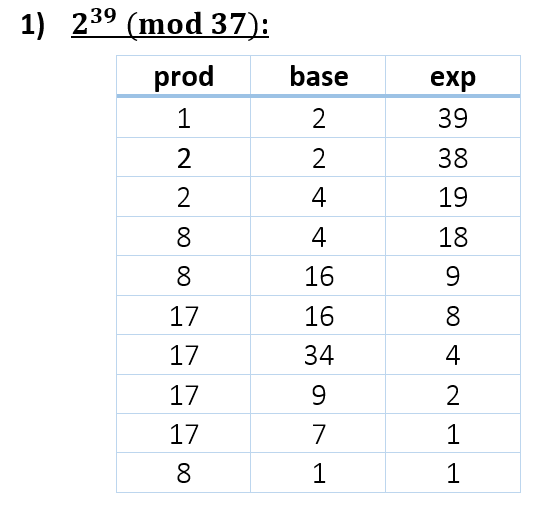
**Assignment 2: Modular Arithmetic and Asymmetric Encryption**

**Task 1 :**

**Task 2 :**

1. **:**

has an inverse in (mod 19) because 12 is a co-prime with 19 :

so now we will find inverse of :

(1)

(2)

(3)

(4)

so inverse of 12 in mod 19 is 8

1. **:**

has an inverse in (mod ) because is a co-prime with :

so now we will find inverse of :

(1)

(2)

(3)

(4)

so inverse of in mod is a

**Task 3 :**



7 is a prime number and is a positive integer not divisible by 7 so :

so

101 is a prime number and is a positive integer not divisible by 101 so :

so

so

**Task 4 :**

has an inverse in (mod 19) because 12 is a co-prime with 19 :

so we looking for :

19 is a prime number and is a positive integer not divisible by 19 so :

therefore :

**Task 5**

The value 65537 in binary is 10000000000000001, which makes it easy to perform calculations using the repetitive squaring algorithm.

We shouldn’t use 3 as an encryption key; this could result in not even cycling once through the value of N (could be too small).

**Task 6**

1. Calculating the private and public keys:

* Alice: . Private key:

The public key for Alice: [65537, ]

and the private key is : [,]

|  |  |
| --- | --- |
| Starting euclid with params: 65537 4001376116572  4001376116572 = 61055222 \* 65537 + 32358  65537 = 2 \* 32358 + 821  32358 = 39 \* 821 + 339  821 = 2 \* 339 + 143  339 = 2 \* 143 + 53  143 = 2 \* 53 + 37  53 = 1 \* 37 + 16  37 = 2 \* 16 + 5  16 = 3 \* 5 + 1  --- Extended: | -3\*37 + 7\*16 = 1  7\*53 + -10\*37 = 1  -10\*143 + 27\*53 = 1  27\*339 + -64\*143 = 1  -64\*821 + 155\*339 = 1  155\*32358 + -6109\*821 = 1  -6109\*65537 + 12373\*32358 = 1  12373\*4001376116572 + -755436267915\*65537 = 1  **Result:**  (-755436267915 mod 4001376116572 =  **)** |

* Bob: . Private key:

The public key for Bob: [65537, ]

and the private key is : [,]

|  |  |
| --- | --- |
| Starting euclid with params: 65537 4002456340132  4002456340132 = 61071705 \* 65537 + 9547  65537 = 6 \* 9547 + 8255  9547 = 1 \* 8255 + 1292  8255 = 6 \* 1292 + 503  1292 = 2 \* 503 + 286  503 = 1 \* 286 + 217  286 = 1 \* 217 + 69  217 = 3 \* 69 + 10  69 = 6 \* 10 + 9  10 = 1 \* 9 + 1 | -1\*69 + 7\*10 = 1  7\*217 + -22\*69 = 1  -22\*286 + 29\*217 = 1  29\*503 + -51\*286 = 1  -51\*1292 + 131\*503 = 1  131\*8255 + -837\*1292 = 1  -837\*9547 + 968\*8255 = 1  968\*65537 + -6645\*9547 = 1  -6645\*4002456340132 + 405821480693\*65537 = 1  **Result:**  (405821480693 mod 4002456340132 =  **)** |

2. Sending a signed message:

* Signature:

M = 726310 (message). Alice creates signature S:

S = M^(alice private key) modulo alice public key [n] =

Calculation:

|  |  |
| --- | --- |
| ('repetitive squaring', 726310, 3245939848657, 4001380117261)  726310 \* 726310^3245939848656  726310 \* 527526216100^1622969924328  726310 \* 3275710919380^811484962164  726310 \* 1320915429712^405742481082  726310 \* 3544132491285^202871240541  3023749799918 \* 3544132491285^202871240540  3023749799918 \* 2380609384776^101435620270  3023749799918 \* 1872132143557^50717810135  2772155859398 \* 1872132143557^50717810134  2772155859398 \* 2900153245441^25358905067  3000276374831 \* 2900153245441^25358905066  3000276374831 \* 1260081418413^12679452533  1354263498311 \* 1260081418413^12679452532  1354263498311 \* 2793090109787^6339726266  1354263498311 \* 132004432939^3169863133  3235185436183 \* 132004432939^3169863132  3235185436183 \* 2633672359193^1584931566  3235185436183 \* 1224120334435^792465783  2734287352707 \* 1224120334435^792465782  2734287352707 \* 2817904173381^396232891  2314963887899 \* 2817904173381^396232890  2314963887899 \* 468156808430^198116445  950939342289 \* 468156808430^198116444  950939342289 \* 3495309084628^99058222  950939342289 \* 2197147277695^49529111  2661142811741 \* 2197147277695^49529110  2661142811741 \* 712079978966^24764555  1251017736062 \* 712079978966^24764554  1251017736062 \* 3421253114060^12382277  3104948212749 \* 3421253114060^12382276  3104948212749 \* 3295294587623^6191138  3104948212749 \* 3762586751377^3095569  54851458274 \* 3762586751377^3095568  54851458274 \* 777407604151^1547784  54851458274 \* 1292611269015^773892 | 54851458274 \* 1740274314611^386946  54851458274 \* 2498605584853^193473  1614895575463 \* 2498605584853^193472  1614895575463 \* 511944915328^96736  1614895575463 \* 3813543421901^48368  1614895575463 \* 2904146040205^24184  1614895575463 \* 3601804612445^12092  1614895575463 \* 3250571987830^6046  1614895575463 \* 2182798997690^3023  2407152478777 \* 2182798997690^3022  2407152478777 \* 2129271524947^1511  225354589234 \* 2129271524947^1510  225354589234 \* 2195588276585^755  112515922930 \* 2195588276585^754  112515922930 \* 1902459596217^377  3862439966761 \* 1902459596217^376  3862439966761 \* 206189406940^188  3862439966761 \* 630910026122^94  3862439966761 \* 3644120009328^47  73948253394 \* 3644120009328^46  73948253394 \* 2997139004288^23  52992621549 \* 2997139004288^22  52992621549 \* 3064259045114^11  1425700943533 \* 3064259045114^10  1425700943533 \* 3552443308010^5  2021120912722 \* 3552443308010^4  2021120912722 \* 3504890017740^2  2021120912722 \* 379746621777^1 |

* Encryption:

M1=726310,M2=

For each:

So for M1:

|  |  |
| --- | --- |
| ('repetitive squaring', 726310, 65537, 4002460341361)  726310 \* 726310^65536  726310 \* 527526216100^32768  726310 \* 2559492956376^16384  726310 \* 614510758293^8192  726310 \* 2500428799326^4096  726310 \* 3854336836170^2048  726310 \* 1062823416641^1024  726310 \* 3873133114286^512  726310 \* 1456028861996^256 | 726310 \* 3541043953635^128  726310 \* 1639351047175^64  726310 \* 3046398623721^32  726310 \* 1725802289081^16  726310 \* 3553575319253^8  726310 \* 2524959410190^4  726310 \* 2706328062940^2  726310 \* 3666179832054^1  ('m,encrypted', 2243156446494L) |

M2 (signature) :

|  |  |
| --- | --- |
| ('repetitive squaring', 123392137971L, 65537, 4002460341361)  123392137971 \* 123392137971^65536  123392137971 \* 2341452371658^32768  123392137971 \* 1138946982804^16384  123392137971 \* 1768451266201^8192  123392137971 \* 3725555181603^4096  123392137971 \* 676188552284^2048  123392137971 \* 2254080063852^1024  123392137971 \* 3591702641304^512  123392137971 \* 1442669259932^256 | 123392137971 \* 3613718089032^128  123392137971 \* 115582342237^64  123392137971 \* 145621708441^32  123392137971 \* 2981644817611^16  123392137971 \* 3667328929362^8  123392137971 \* 2964461708408^4  123392137971 \* 2279207865268^2  123392137971 \* 3804593812518^1  ('s,encrypted', 1472006170868L) |

* Decryption: Bob uses his private key [,] for each message M from cipher as such:

:

|  |  |
| --- | --- |
| ('repetitive squaring', 2243156446494L, 405821480693, 4002460341361)  2243156446494 \* 2243156446494^405821480692  2243156446494 \* 3976602667557^202910740346  2243156446494 \* 1431885480424^101455370173  2797322633882 \* 1431885480424^101455370172  2797322633882 \* 2055406857949^50727685086  2797322633882 \* 2898434109091^25363842543  847818232728 \* 2898434109091^25363842542  847818232728 \* 617162555092^12681921271  1683801295596 \* 617162555092^12681921270  1683801295596 \* 3917244106875^6340960635  3465845807277 \* 3917244106875^6340960634  3465845807277 \* 2849312599633^3170480317  1836255715704 \* 2849312599633^3170480316  1836255715704 \* 3878020029997^1585240158  1836255715704 \* 2308052875749^792620079  908034503607 \* 2308052875749^792620078  908034503607 \* 2770762511788^396310039  1458474598554 \* 2770762511788^396310038  1458474598554 \* 3569717216512^198155019  2679261886349 \* 3569717216512^198155018  2679261886349 \* 1276177491911^99077509  2621382477185 \* 1276177491911^99077508  2621382477185 \* 3677621087916^49538754  2621382477185 \* 2144521934701^24769377  3065093356652 \* 2144521934701^24769376  3065093356652 \* 425852594445^12384688  3065093356652 \* 3377615218213^6192344  3065093356652 \* 3266786609901^3096172  3065093356652 \* 10603550374^1548086  3065093356652 \* 1753739012575^774043  3260674677776 \* 1753739012575^774042 | 3260674677776 \* 1222708163328^387021  2467436334048 \* 1222708163328^387020  2467436334048 \* 965256003833^193510  2467436334048 \* 53615783123^96755  222871427753 \* 53615783123^96754  222871427753 \* 2366116588327^48377  2900169881000 \* 2366116588327^48376  2900169881000 \* 2063718684910^24188  2900169881000 \* 3912695019888^12094  2900169881000 \* 3177871463194^6047  1636385645212 \* 3177871463194^6046  1636385645212 \* 2947248549049^3023  3840769527410 \* 2947248549049^3022  3840769527410 \* 306519570660^1511  2927017257781 \* 306519570660^1510  2927017257781 \* 1343959746790^755  3345337848416 \* 1343959746790^754  3345337848416 \* 359013237980^377  3798753389098 \* 359013237980^376  3798753389098 \* 1901353262181^188  3798753389098 \* 1723821373935^94  3798753389098 \* 1187153013800^47  2337549245632 \* 1187153013800^46  2337549245632 \* 3468200452067^23  3748614794813 \* 3468200452067^22  3748614794813 \* 1152872091719^11  1274662580203 \* 1152872091719^10  1274662580203 \* 1388794173845^5  1286768791291 \* 1388794173845^4  1286768791291 \* 3737194237974^2  1286768791291 \* 3358363722687^1 mod 4002460341361 = 725310  ('m,decrypted', 726310) |

|  |  |
| --- | --- |
| ('repetitive squaring', 1472006170868L, 405821480693, 4002460341361)  1472006170868 \* 1472006170868^405821480692  1472006170868 \* 3580173030343^202910740346  1472006170868 \* 2772700779002^101455370173  2257357880165 \* 2772700779002^101455370172  2257357880165 \* 3125635867858^50727685086  2257357880165 \* 3956633777020^25363842543  1142166510331 \* 3956633777020^25363842542  1142166510331 \* 602321045394^12681921271  3341127843250 \* 602321045394^12681921270  3341127843250 \* 1420558453394^6340960635  2651445491018 \* 1420558453394^6340960634  2651445491018 \* 2607855599061^3170480317  1048896457672 \* 2607855599061^3170480316  1048896457672 \* 3456999658899^1585240158  1048896457672 \* 3168790063552^792620079  2725080149950 \* 3168790063552^792620078  2725080149950 \* 2918147143142^396310039  3188063510505 \* 2918147143142^396310038  3188063510505 \* 3018112937626^198155019  2994894586809 \* 3018112937626^198155018  2994894586809 \* 3995901089556^99077509  1339512393498 \* 3995901089556^99077508  1339512393498 \* 1210352354451^49538754  1339512393498 \* 3030053779118^24769377  2297874685449 \* 3030053779118^24769376  2297874685449 \* 1755296166793^12384688  2297874685449 \* 550236874666^6192344  2297874685449 \* 1329102731642^3096172  2297874685449 \* 51476560838^1548086  2297874685449 \* 2134030280784^774043  1960177924274 \* 2134030280784^774042 | 1960177924274 \* 1945222561326^387021  498068729259 \* 1945222561326^387020  498068729259 \* 2776018151276^193510  498068729259 \* 180461568400^96755  2359603099927 \* 180461568400^96754  2359603099927 \* 1162275151080^48377  2954084235407 \* 1162275151080^48376  2954084235407 \* 1874569168648^24188  2954084235407 \* 780322747596^12094  2954084235407 \* 553409566854^6047  180557915256 \* 553409566854^6046  180557915256 \* 528589823375^3023  1118315494867 \* 528589823375^3022  1118315494867 \* 1228217055729^1511  2477771535073 \* 1228217055729^1510  2477771535073 \* 2182905187068^755  960373347059 \* 2182905187068^754  960373347059 \* 2966667938390^377  2418656448726 \* 2966667938390^376  2418656448726 \* 3856994119219^188  2418656448726 \* 3735726487145^94  2418656448726 \* 75644861446^47  742252960234 \* 75644861446^46  742252960234 \* 3171586804572^23  2051041432512 \* 3171586804572^22  2051041432512 \* 2421524391062^11  3618871855497 \* 2421524391062^10  3618871855497 \* 348665919184^5  3937541148761 \* 348665919184^4  3937541148761 \* 1536685931787^2  3937541148761 \* 3352534746314^1 mod 4002460341361 = 123392137971  ('s,decrypted', 123392137971L) |

* Bob verifying: uses e from the public part of the key ->

|  |  |
| --- | --- |
| ('repetitive squaring', 123392137971L, 65537, 4001380117261)  123392137971 \* 123392137971^65536  123392137971 \* 3823980066442^32768  123392137971 \* 2744222180823^16384  123392137971 \* 933683911594^8192  123392137971 \* 1055308717864^4096  123392137971 \* 3150619341643^2048  123392137971 \* 3855210321967^1024  123392137971 \* 1424304194137^512 | 123392137971 \* 2080342642234^256  123392137971 \* 2492040006013^128  123392137971 \* 2989619430527^64  123392137971 \* 3295576111307^32  123392137971 \* 3370454441381^16  123392137971 \* 3926370448911^8  123392137971 \* 1238303036009^4  123392137971 \* 2492475875860^2  123392137971 \* 1588044145692^1  123392137971 \* 1588044145692 mod 4001380117261 **= 726310** |

So to verify the message, we only need the public part of the key.

3. In every calculation, there’s a table with the included calculation performed in Python. (code added as an appendix)

**Task 7**

Assuming 67 is one of the primes used for N->

So the key uses the primes 53,67. To find the private key, we just need to calculate the inverse of e=1565 in- which is 125; Having the primes creating the public key makes this a trivial calculation:

|  |  |
| --- | --- |
| Starting euclid with params: 1565 3432  3432 = 2 \* 1565 + 302  1565 = 5 \* 302 + 55  302 = 5 \* 55 + 27  55 = 2 \* 27 + 1 | --- Extended:  -2\*302 + 11\*55 = 1  11\*1565 + -57\*302 = 1  -57\*3432 + 125\*1565 = 1  **Result: 125** |

so the private key is: (d = 125, n = 3551)

**Task 8**

1. Alice sent Bob the value . Bob needs to send Alice the value

|  |  |
| --- | --- |
| repetitive squaring 2 871 1373  2 \* 2^870  2 \* 4^435.0  8 \* 4^434.0  8 \* 16^217.0  128 \* 16^216.0  128 \* 256^108.0  128 \* 1005^54.0  128 \* 870^27.0 | 147 \* 870^26.0  147 \* 377^13.0  499 \* 377^12.0  499 \* 710^6.0  499 \* 209^3.0  1316 \* 209^2.0  1316 \* 1118^1.0  = 805 |

2. Their secret key:

|  |  |
| --- | --- |
| repetitive squaring 974 871 1373  974 \* 974^870  974 \* 1306^435.0  646 \* 1306^434.0  646 \* 370^217.0  118 \* 370^216.0  118 \* 973^108.0  118 \* 732^54.0  118 \* 354^27.0 | 582 \* 354^26.0  582 \* 373^13.0  152 \* 373^12.0  152 \* 456^6.0  152 \* 613^3.0  1185 \* 613^2.0  1185 \* 940^1.0  = 397 |

3. We can try an get Alice’s key by computing exponents of 2 mod 1373 until we find it - (side note: in the worse case, we only have 1372 options). We end up finding that a=587.