

به نام خدا

مهدی سعیدی – 401207254

پروژه درس رمزنگاری

سوال 3

(آ)

در قضیه باقی مانده چینی اینگونه گفته میشود که اگر ما تجزیه  $N$  را بدانیم که ممکن است بدانیم چون کلید خصوصی  $(d)$  را داریم آنگاه میتوان  $M$  را به دو قسمت تقسیم کرد یکی همنهشتی به پیمانه  $q$  و یکی همنهشتی به پیمانه  $p$  هر کدام را سوا حساب کرد و سپس دوباره ترکیب کرد. به این گونه که :

$$N = p * q, \gcd(p, q) = 1$$

$$\gcd(d, \Phi(N)) = 1 \rightarrow \gcd(d, p-1) = 1, \gcd(d, q-1) = 1$$

برای امضا باید بتوانیم  $m^d$  را به پیمانه  $N$  حساب کنیم.

$$d \equiv d_p \pmod{p-1 = \Phi(p)}$$

$$d \equiv d_q \pmod{q-1 = \Phi(q)}$$

$$m^{d_p} \equiv x \pmod{p} \Leftrightarrow m^d \equiv x \pmod{p} *$$

$$m^{d_q} \equiv y \pmod{q} \Leftrightarrow m^d \equiv y \pmod{q} **$$

$$*, ** \Leftrightarrow m^d \equiv xq + yp \pmod{p*q}$$

$$\Leftrightarrow m^d \equiv xq + yp \pmod{N}$$

که همین مقدار از طرف قضیه باقی مانده چینی بدست می آید و چون همه روابط دو طرفه و برگشت پذیر هستند قضیه درست است.

برای حل قسمت الف از لینک زیر کمک گرفته شده است.

<https://crypto.stackexchange.com/questions/2575/chinese-remainder-theorem-and-rsa>

(ب)

بعد از چک کردن تک تک امضا ها مشاهده میشود که  $\text{sig3}$  دارای خطا بوده و بعد از طبق مقاله میتوانیم با داشتن  $\text{sig3}$  غلط و پیام  $m$  و با فرض  $N=p*q$  میتوان  $q$  را حساب کرد و با توجه به  $q$  میتوان  $p$  را حساب کرد و در نتیجه  $\Phi(N)$  و در نهایت  $d$  که مسئله هم همین را از ما خواسته و در نوت بوک گام به گام نشان داده شده که چگونه این مراحل انجام شده است.

در پایین فقط نتیجه را آورده ام.

$$q = \gcd(\text{sig3} - m, N)$$

$$p = N/q$$

$$\Phi(N) = (p-1)*(q-1)$$

$$d \equiv e^{-1} \bmod \Phi(N)$$

q=313412290387493142447972589196376369164419559068364026729716  
18438862383882051262592032888744453189634620931974910432931959  
70567528949716610918051532549767483693300833160590891625763991  
73121694150060764539764684162776662768767497042850082914372075  
47081351658150492520813841414148957843427724035033708078507670  
80841689731459970227706173255875367077249836623893271072630697  
91370552028823487782791506976912628491119456325936155190755134  
77823782408815406831006117927964077578537687042065535210335664  
16663880662361908148766821730024703227663370616839793589690947  
8271849375578808644196740939370935488580037218350664830977701

p=309531054862077701101289385209368706555230231964330680343610  
51671457763190570433443983536656599259247450895709471949832215  
47433721421969743815728169265363592439033583172076829529663043  
83894481470527195401382461329049175680133660502329506418587397  
77063386433253172579014592368010200148490857617749225138818318  
84262950808034010211323486956286892816094157004501677745522822  
56446174669294712207964235172823078774053750872669851128768673  
49485987537356060416253221135843057506100224740988203274140265  
04243165626738328650814459088912093336101180936971767378701804  
6408502901215802100543929292065468690675654619841973561378829

$\Phi(N)=$ 701083685038056759383292130228643028079965784372036392485  
83177679721468801381573324408354292760440129889027342891743295  
54782662171277202258406910751642314682091986555684912205772654  
45405010008272208386892953903299007526396924657650051798911855  
71337866177821965719745153089989439299847479341476500219640125  
26270294131687150170737083181510831472531657990054748314462401  
11083608368652670975477071316216639850351724516852835070903523  
52908931422129657830247728462203079220531706888828065225384084  
08873381757676294652825962452829282143672454128551931486558947  
46373624781452933752792768231046543940286516812404561901710090  
27595231133435760411325124888492273232150992495906386314203654  
08179141075606854302432108286419901445965656396986813530460750  
02048598215800622180301456360601922835098897289707285907033142  
73581563870698738681233055342908110174299656062285620901475830  
94904524415952432268060779536341329678661732724718807084669699  
61038539441981430425922863077975248013867432606148090144957502  
99931078886174894151940787599272657815074579635212682983219748  
18984376750134702090014999821869680877259426474689845402178740  
28724616744343926910501652062262613759556106941663328169716350  
89227856630840180543473141212498979444805402837179320135600

d=513704332217771215920224865476684663085718193662888369874770  
44414906165758705992219128534304859786554568669308799174602634  
68235512751581590820076339663083279258007387320886206553754673  
19736129708529105480466106565892178763261780855222847596681326  
08616976418105037365207123968130218749571880108336456692236304  
86113626723943512100431412379498444272302148232082618223451131  
65151814739341583430667078074953490954127054385859572913981232  
82041527798934411616212473186590263926228475319116187164089375  
79599066967359094300429072070719452391792190788815829698554576  
47054754437253174476891265529760686182924576129038430561281372  
25788335222476813578020254406267986402441435491302974881553338  
19749014889085969317490709022256526512950149688008875537650287  
18272964098363965615120834854096357888325879338391519474004280  
79366758577183922354566050658838603367403549118147287432774214  
95592742010182354137023807969833079280828802781087753584047568  
97449490813622169921154523792747619014076599728036560096747156  
70244536164019602131548732540638596234719641821293239314674368  
95240567521666694129851158609892740229810849409701992519051837  
78413872309858003115872458563501148834452500577512154663527841  
319613905376773816022886196172613678571291027381038588673