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.

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

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

$m^{d_p} \equiv x \ (\mathrm{mod}\ p) \Leftrightarrow m^d \equiv x \bmod p$ *

$m^{d_q} \equiv y \ (\mathrm{mod}\ q) \Leftrightarrow m^d \equiv y \bmod q$ **

* , ** $\Leftrightarrow m^d \equiv xq + yp \ (\mathrm{mod}\ p*q)$

$\Leftrightarrow m^d \equiv xq + yp \ (\mathrm{mod}\ N)$

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 sig3 دارای خطا بوده و بعد از طبق مقاله میتوانیم با داشتن 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 Φ(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.

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

$p = N/q$

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

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

q=3134122903874931424479725891963763691644195590683640267297161843886238388205126259203288874445318963462093197491043293195970567528949716610918051532549767483693300833160590891625763991731216941500607645397646841627766627687674970428500829143720754708135165815049252081384141414895784342772403503370807850767080841689731459970227706173255875367077249836623893271072630697913705520288234877827915069769126284911194563259361551907551347782378240881540683100611792796407757853768704206553521033566416663880662361908148766821730024703227663370616839793589690947827184937557880864419674093937093548858003721835066483097701 p=30953105486207770110128938520936870655523023196433068034361051671457763190570433443983536656599259247450895709471949832215474337214219697438157281692653635924390335831720768295296630438389448147052719540138246132904917568013366050232950641858739777063386433253172579014592368010200148490857617749225138818318842629508080340102113234869562868928160941570045016777455228225644617466929471220796423517282307877405375087266985112876867349485987537356060416253221135843057506100224740988203274140265042431656267383286508144590889120933361011809369717673787018046408502901215802100543929292065468690675654619841973561378829 d=513704332217771215920224865476684663085718193662888369874770444149061657587059922191285343048597865545686693087991746026346823551275158159082007633966308327925800738732088620655375467319736129708529105480466106565892178763261780855222847596681326086169764181050373652071239681302187495718801083364566922363048611362672394351210043141237949844427230214823208261822345113165151814739341583430667078074953490954127054385859572913981232820415277989344116162124731865902639262284753191161871640893757959906696735909430042907207071945239179219078881582969855457647054754437253174476891265529760686182924576129038430561281372257883352224768135780202544062679864024414354913029748815533381974901488908596931749070902225652651295014968800887553765028718272964098363965615120834854096357888325879338391519474004280793667585771839223545660506588386033674035491181472874327742149559274201018235413702380796983307928082880278108775358404756897449490813622169921154523792747619014076599728036560096747156702445361640196021315487325406385962347196418212932393146743689524056752166669412985115860989274022981084940970199251905183778413872309858003115872458563501148834452500577512154663527841319613905376773816022886196172613678571291027381038588673