به نام خدا

مهدی سعیدی – 401207254

پروژه درس رمزنگاری

سوال 1

آ)

برای قسمت من از سایت https://neuromancer.sk/std/secg/secp192r1 استفاده کردم و همچنین میتوان از کتابخانه tinyec نیز استفاده کرد که در نوت بوک فرستاده شده کد ان قرار دارد. فرمول خم به صورت زیر است:

$$y^2 = x^3 + ax + b \mod p$$

که مقادیر a , b ,p هم به فرم hex و هم به فرم عادی در زیر نوشته شده است.

a = 0xfffffffffffffffffffffffffffffffefffffffffffffffc

a = 6277101735386680763835789423207666416083908700390324961276

---

b = 0x64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

b = 2455155546008943817740293915197451784769108058161191238065

---

p = 0xfffffffffffffffffffffffffffffffeffffffffffffffff

p = 6277101735386680763835789423207666416083908700390324961279

که اگر a,b,p را در فرمول بالا جای گذاری کنیم معادله کلی خم بدست می آید.

"secp192r1" =>
y^2 = x^3 +
6277101735386680763835789423207666416083908700390324961276x +
2455155546008943817740293915197451784769108058161191238065 (mod
6277101735386680763835789423207666416083908700390324961279)

ب)

در این قسمت از تابع nthroot_mod همانطور که در نوتبوک تمرین ششم وجود داشت استفاده کریم با استفاده از کتابخانه sympy و در اولین تلاش نقطه رو خم پیدا شد.

(x, y) = (401207254, 3075002300464187516527786225381035405128256020931106480378)

پ)

2G = (46458418636543854238084358783302348355719068252631861263 91 ,
38278246165136235787984055818363800654951981844797066070 98)
s.G = (12412702764367624643636615300179968610921029412437940 14800 ,
11775406651216202863849923316070631976757698512332320933 96)

ت)

برای رمزکردن در الجمال نفر اول یک عدد رندوم انتخاب میکند (k) که به عنوان کلید خصوصی نیز استفاده میشود. سپس k*G به عنوان کلید عمومی به نفر دوم گفته میشود. نفر دوم یک مقدار تصادفی دیگر انتخاب میکند به اسم r و پیام رمز شده رو را میسازد. در این سیستم رمزنگاری باید r, k بین 1 تا n-1 باشند که در اینجا n همان order گروه است. در این خم co-factor =1 و تمام نقاط رو خم مولد بوده و n برای همه یکی و برابر

Group order (n) is 6277101735386680763835789423176059013767194773182842284081

است .

Cipher = (r*G , r*k*G + m)

```
(Private key) k =  128474557739267279152015414560704653996393582308993759039 3
Public key (k.G) = ( 39532727376634160458106077760463146542615253895457062171 63  ,  38929850359430813028977078675445813386883670299769703327 33 )
Group order (n) is 627710173538668076383578942317605901376719477318284228408 1
```

ث)برای رمز گشایی که نفر اول k (عدد اول رندوم انتخاب شده) را دارد.در نتیجه طبق فرمول:

Cipher = (x, y)

message = y – k*x = (r*k*G + m) – k*r*G = m