SKYDAYS CTF - Crypto - SKYSECC Write-up

Hazirlayan: s4g0l4nd1n

Verilen kodu inceledigimizde bize bir Elliptic Curve'e ait iki public key point'i ve g point'i verilmis. Bizim bunlari kullanarak bu Elliptic Curve'u olusturmak icin kullanilan p asal sayisina ve b degerine ulasmamiz gerekiyor.

Bunun icin "y**2 = x**3 + a*x + b mod p" Elliptic Curve genel denklemi ile elimizdeki 3 adet noktayi kullanarak 3 adet denklemle karsilasiriz.

Bu denklemler ile sirasiyla 1.den 2. ve 1.den 3.yu cikarip b degerinden kurtuluruz ve daha sonra elimizde Ya**2 - Yb**2 ve Ya**2 - Yg**2 degerlerinin esitlikleri olusur.

Ardindan bu denklemlerde esitligin sag tarafinda kalanlar sola aktarilir ve 2 denklem de 0'a esitlenir. Daha sonra bu denklemler sage koduna uygulanip iki farkli degiskene atanir. Sonrasinda GCD metodu ile p degerine ulasiriz. Buldugumuz bu p degerini genel denklemde kullanarak da b degerini elde ederiz.

Daha sonra soruda n degerine eklenen hash'li kisim icin sorudaki kodu kullaniriz ve bu degeri outputta verilen n degerindan cikararak gercek n degerine ulasiriz.

Artik flag'e ulasmak icin RSA ile sifrelenmis kisim kaliyor. Bunun icin de verilen koddaki generatePrime fonksiyonunu biraz incelememiz ve asal sayiyi nasil olusturdugunu anlamamiz gerekiyor.

Anlasildigi uzere random integerin karesini alip 1 ekliyor ve prime olup olmadigina bakiyor. Eger prime ise bu sayiyi donduruyor. Yani n degeri r*q'ya o da (x**2 + 1) * (y**2 + 1) degerine esit oluyor. Burdan da "near square RSA primes" metodu ile phi degeri icin (x**2) * (y**2) degerini kullanabilecegimizi buluyoruz.

Bu deger ile private exponent'i de bulup flag'e ulasiyoruz.

Flag: **SKYSEC{RS4_1y1ydi_y4_3ll1pT1c_CurV3_d3_n3rd3n_c1kT1_51mD1_??}**