SKYDAYS CTF - Crypto - RSA Math Write-up

Hazirlayan: s4g0l4nd1n

Soruda bize output olarak A, B, x+y, c1, c2 ve (C * A) + (2 * k) degerleri verilmis. Buradan anlasildigi uzere elimizde iki farkli sifreli metin var yani flag ikiye bolunmus ve bu iki parca ayri ayri sifrelenmis.

Flag'in ilk parcasi icin verilen kodu inceledigimizde public exponent'i bulmamiz gerektigini anlariz. Bunun icin (C * A) + (2 * k) ifadesini kullanmamiz gerekir. Bu degerin A degeri ile bolumunden kalaninin (2 * k) oldugunu buluruz. Ardindan bu degeri de 2'ye bolerek k yani public exponent'e ulasiriz.

Phi degeri icin ise x+y ifadesini kullanmaliyiz. Elimizde A degeri oldugu icin bu degerden x+y'yi cikarip 1 eklersek phi degerine ulasmis oluruz.

Sonunda bu iki ifadeyi kullanip 1. private exponent, ardindan da flag'in ilk kismina ulasiriz.

Flag'in ikinci kismi icin ise verilen kodu inceledigimizde B degeri, olusturulan random asal sayinin kupu alinarak olusturulmus. Bunun uzerine B'nin 3. dereceden kokunu aliriz ve z'yi buluruz.

Bundan sonra geriye phi degerini bulmak kaliyor. Bunun icin ise ufak bir arastirma ile bu phi degerine ulasmak icin Euler's Totient formulunun kullanilmasi gerektigini anlariz ve bu durumda bizim phi degerimiz (z**2) * (z-1) degerine esit olur.

Phi degerini de bulduktan sonra once 2. private exponent, ardindan da flag'in 2. kismina ulasiriz.

Flag: **SKYSEC{s4d3c3_b1r4z_m4tem4T1k_g3R1s1_k0l4y_z4t3n_d1m1_AB1_<3}**