به نام خدا

مهدی سعیدی – 401207254

پروژه درس رمزنگاری

سوال 2

طبق لینک ویکی پدیا سیستم رمزنگاری paillier cryptosystem فرمول رمزگذاری و رمزگشایی طبق زیر است:

رمزگذاری:

$$c = g^m \cdot r^n \bmod n^2$$

رمزگشایی:

$$L(x) = \frac{x-1}{n}$$

$$m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$$

که طبق متن صورت سوال یک 1- کم است.

حال در اینجا به بعد طبق فرمول ویکی پدیا پیش میرویم.

آ) طبق خواص homomorphic این سیستم در صورت داشتن دو cipher متوان رمز شده جمع palan-text های متناظر آن ها را بدست آورد. طبق homomorphic addition of palintext . به این صورت c1 , c2 را در هم ضرب کرده و mod $n^2$ میگیریم.

c1 = 14311352900693250085830057677604401943522506698686420156372846648278630965268542952902131631967806727782287211280522340928774697823432044408190883452266 74

c2 = 766502765098026355380112715536128541917607723218993231191798626637402444561652254317663096357141828249072007319292850196436742539757315839907222753619573

n = 611869294362308554207663795009463779039315416992025512254662670013109074097 61

Enc(m1 + m2) = 344247984484960101592911642022533117476234750378634702848827015878284524608729069455579613051587200595986114024601257088317245288251069759932353719834121 2

ب)

برای محاسبه این قسمت طبق قسمت Background در لینک ویکی و پدیا و اینکه با داشتن $r^n$ چون n که معلوم است و r را در این قسمت سوال به ما داده است ما میتوانیم معکوس $r^n$ را حساب کنیم با الگوریتم اقلیدسی تعمیم یافته . و معکوس $r^n$ میشه $g^m$ و از اینجا طبق background ویکی پدیا میشود m mod n را بدست اورد.

c = 185785543343525396626147240556463006820725743559936765242230229117734655786087381668009860208349623634956838525426286375816615379836274402305873253869677 8
r = 149351277470671413322664390782274263122356597273772653980120656211018407122 18
n2 = 707000635345465143420612403505488642277226337155935604768689145100924412927 83
m = math.floor((g_topow_m - 1) / n2)
m = 73313