Homework 7

1.

4G = (103388573995635080359749164254216598308788835304023601477803095234286494993683, 37057141145242123013015316630864329550140216928701153669873286428255828810018 )

2.

5G =

(21505829891763648114329055987619236494102133314575206970830385799158076338148, 98003708678762621233683240503080860129026887322874138805529884920309963580118)

3.

d = 902027

Q =

(74126695233396451170897216802809900713995848088865862928203296249783989218958, 21228009354059859483409810275841212215869119722716887978142090737871868810027)

d = 902028

Q =

(19292789413885822208795898529305149840182528658437072379106007877942422663179, 85523802914842987620789296500568519676390717070621931282164943219424747867739)

4.

5.

902027 = 1101 1100 0011 1000 1011 (in binary)

# of Additions = 10

# of Doubles = 19

6

z = 10

k = 66666

d = 902027

1. kG = ()
2. r = x1 mod 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

= 29930184684980401757111440714186039316228031672971230850124573730964070201374

1. s = k^-1 (z+rd)

= 24655277153627087181435666339638269162257060944731471330379508156989324429426 \* (10 + 29930184684980401757111440714186039316228031672971230850124573730964070201374\* 902027) mod 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141 =

63855085458334682923006652616008722758963221534974104921968626568340826553505

z = 10

k = 77777

d = 902028

encrypted:

7.

(1) w= s-1 mod n = 96034977103095801461015162728158047602408667036161711509265724500744428699417

(2) u1 = zw mod n = 34013057132428451221583747212077213201386156129017880031815939875298995039474

U2 = rw mod n = 75425210646516160345521931566186506475033461021241132832491861192217667869973

(x1,y2) = u1 \* G + u2 \*Q = (29930184684980401757111440714186039316228031672971230850124573730964070201374, 42095718535045239447971676092147938700704502177014755608259441262637977869612

)