SAMPLE INPUT – OUTPUT

.....DIGITAL SIGNATURE STANDARD.....

.....Generating Public Key.....

.....Generating Private Key.....

Public Key :
p :
17976931348594544714775252644472179417393481454794911506106311048574461633193503
86623223273535185107338927317176238755464951402279961225263467211335355259720928
77704279342109336571338638324661946388175413191271142685271620423599897616686531
27001081767193165223783835553304035051785993564549779851042136592290 3

q :
14615016373285766069517844019059295864355479920 63

g :
35570445675624733492968046178529371799720267837486730895765449530668375863738110
44722795793019615784828199313166963629410266906075695456323660151305807783544008
94213216306080330218447352343034100292880915278267775072240184973514836375895291
57559511993903277928594874503711058200546701132349743330205088816870

y :
16339644440384695780453739154543992866634703745405801008444213890348816232417692
77984196154148379168161101130441838881796652005322433198878263604690129209796581
49466433826611779311809389206002812650689955632330925199827644217873968937757935
11013011423754352106873317780188907247069371694179024388397664440 2935

Enter message to sign :
message

Generating a random value k :
66408213029486433006954943451865958863075776935 1

Private Key
x :
13674030605271492785560303576742846080211996708 40

Hashed Value :
90750528098856413967761560964454263353649541365237564892585272301200766142595670
92106775697330294837434866930877520331579709138450193408424372420452639972830637
48398486018764109512735923281481590852618759303265273264501260393164463572037713
79667457463978934547903546874178452357261848365816349104579643616486067219948242
78185502791416573744788473108358636335141495544805566928887218176

Signature
r :
12689938231361344532405833598384867335252609527 35

s :
133069058939182537418572756715943529413030572323

Verification :
Enter message :
message

Enter the values of Signature for verification :
r : 126899382313613445324058335983848673352526095273 5

s : 133069058939182537418572756715943529413030572323

r :
126899382313613445324058335983848673352526095273 5

s :
133069058939182537418572756715943529413030572323

Hashed Value :
907505280988564139677615609644542633536495413652375648925852723012007661425956709210677569733029483743486693087752033157970913845019340842437242045263997283063748398486018764109512735923281481590852618759303265273264501260393164463572037137966745746397893454790354687417845235726184836581634910457964361648606721994824278185502791416573744788473108358636335141495544805566928887218176

The signature are matching....Verified
r :
126899382313613445324058335983848673352526095273 5

v :
126899382313613445324058335983848673352526095273 5

Exit (Yes : 1 | No : 0)
0
Enter message to sign :
qwertyuiopasdfghjkl

Generating a random value k :
144063820228566986010016648137637893915467859456

Private Key
x :
136740306052714927855603035767428460802119967084 0

Hashed Value :
19564182516291107702054698254164481406891005605905915733392490188033631077396701
36420327759266289402498486331348601838406876866006008255296586776056521850130723
51253819730639407423931174489994740025473700119199923815399504541752861331064024
66282511277014825617990302914722041257353047474877668993287524701110726980811278
56737670714230323195515570377336397639182436518950636829667858841 6

Signature
r :
81510923897891518041957803801878209690735485043 6

s :
12139321600158563956758016335003258432931584551 70

Verification :
Enter message :
qwertyuiopasdfghjkl

Enter the values of Signature for verification :
r : 81510923897891518041957803801878209690735485043 6

s : 12139321600158563956758016335003258432931584551 70

r :
81510923897891518041957803801878209690735485043 6

s :
12139321600158563956758016335003258432931584551 70

Hashed Value :
19564182516291107702054698254164481406891005605905915733392490188033631077396701
36420327759266289402498486331348601838406876866006008255296586776056521850130723
51253819730639407423931174489994740025473700119199923815399504541752861331064024
66282511277014825617990302914722041257353047474877668993287524701110726980811278
56737670714230323195515570377336397639182436518950636829667858841 6

The signature are matching....Verified
r :
81510923897891518041957803801878209690735485043 6

v :
81510923897891518041957803801878209690735485043 6

Exit (Yes : 1 | No : 0)
1