**Bài tập 6**

**Phạm Văn Nam**

**MSSV: 20183599**

**Báo cáo kết quả**

Bài 1:

p = 134078079299425970995740249982058461274793658205923933\

777235614437217640300736627688911116143623269986750405460\

94339320838419523375986027530441562135724301

q = 13407807929942597099574024998205846127479365820592393377\

72356144372176403007377856098034893055775056966004923400\

2192590823085163940025485114449475265364281

Bài 2:

p = 25464796146996183438008816563973942229341454268524157\

84632858192788577796998522283514385107324957345410738\

4461557193173304497244814071505790566593206419759

q = 2546479614699618343800881656397394222934145426852415\

78463285819278857779701063980544912465269708141676325\

63509541784734741871379856682354747718346471375403

Bài 3:

p = 2190984959247553309227398853158395589898217609334492\

903009942358412721207812615004472110257095781266512\

7475051465088833555993294644190955293613411658629209

q = 328647743887132996384109827973759338484732641400173935\

451491353761908181171892400358258164949547118216260762\

10364113848440012285863311027426121370050758081

Bài 4:

d = 1590128797899941302944410362238731766907763942037101\

362915718114151359265215856818472701290365881352849103\

79105475218548159311649996413081859765873862893558666\

786159443196819394738421950922073770982699963463537441\

0954901130658130263935313668458679622922107175541052773\

4011645528084075140176976118813890397473

plain = 142645187985621451033064600240099557836700899647211\

47486130755572225610557951157288911779615430083155039159\

6369704021295660685265917467899548615443041061347568393\

11675584068948557297466911281227530132812277925855567187\

3541791405921467050482702503673739014327885092286007524\

6427162405295463406302195816284462

Đổi bản rõ sang cơ số 16, ta được:

20805907610B524330594E51D5DBBF643F09603731E9817111392D0C64E2739959A092D4DAF979D387520EA7E577AF9EB50A29F736925E810AB2FB4640E091A0F73252CB669D5B62B26764190ED188239FE71E1A7CB9E935D2DB55C98B024E1DAE46D00466163746F72696E67206C65747320757320627265616B205253412E

Loại bỏ phần padding, ta được phần thông điệp là:

466163746F72696E67206C65747320757320627265616B205253412E

Thông điệp là:

Factoring lets us break RSA.