



## Du RSA très sécurisé ?

Cette énigme a été créée par **jaudi**

Votre état-major a, lors d'une nouvelle opération commando, intercepté des documents confidentiels récupérés sur un espion ennemi et vous les a confiés pour que vous essayez d'en décrypter le contenu.

DOSSIER n°449-A :

Message chiffré envoyé par l'espion et intercepté par nos agents :

C =

17488325840220943611363447689137498897289564788031175034479  
10275254394096303832564372626660864815603395329375930794272  
40129175972787586849616128819663111610679739692486184131345  
63634622354406014892080559252842839907653630589154023491423  
27737482008096039604019633116056323738055069724655191524185  
02290187256772512150993413180014446625595458971289930616747  
09494062162425643064816692478354691747537735697446000793406  
08836585549160846615492082148411395351615415333568622270315  
76535140869583921725001494680364111528258898377179465097625  
90253294652749659967024560712095507820796875619840408859097  
74698877460944206555011661

DOSSIER n°449-B :

Clé publique (N,e) de l'espion trouvée dans les bases de données :

N =

14674586647926905537460474990991631393939381731521675145002  
13955281521957860680280727386216576518670419053410494192379  
90105388478752350019398907335368739035035924346527603331129  
66520390642945627286946447077269288880493088504290500467678  
95048335694348755012442849553005837433500841153862263102138  
37101321456876225152821553295484370994445428304843377412363  
48001514534690633914365340097808081324812275323596740939092  
56624470763924153794948949747345876396280069552968908882030  
25078246236095695410849201940091631529793266409199704969618  
18466510409336299486890331344464195193034720994485649083664  
923640438348866203529022809

e =

85858273718117435595149022258653100028889541293103531960030  
56040389335524238362670452892881167873852585946104269061958  
97331772074753496728662504948606745585290197254674120644903  
42618148184511887930554557376305815256171271486187782607098  
65376419919484175828805763264200099332920252286900275208799  
01714502720058735122397559519966098185945472480921883116397  
80123924813870915555720738787446859295416795517633800263806  
88213887081186983901620800970280047829424602355445857577192  
02184322420781646521233882804273332524215093413746064124840  
16255158778613522938660284708284803988505859743647412932497  
71635658247567265918043043

DOSSIER n°449-C :

Note du service du chiffre de l'état-major

Après une étude du système, il semblerait que la clé publique N est trop grande (d'environ 2048 bits, ce qui correspond au standard de sécurité actuelle pour les banques et les gouvernements), donc le déchiffrement paraît difficile. Néanmoins, comme e est très grand, il se pourrait que sa génération ait été biaisée et ne suive pas les standards de sécurité en vigueur...