



Du RSA ultra-sécurisé !

Cette énigme a été créée par **jaudi**

Votre état-major poursuit le démantèlement d'un réseau de trafiquants ennemis et vient à présent de fouiller un de leurs entrepôts dans lequel il a trouvé de nouveaux codes secrets, qu'il vous confie pour que vous essayez d'en décrypter le contenu.

DOSSIER n°454-A :

Message chiffré retrouvé dans une cache de l'entrepôt désaffecté et intercepté par nos agents :

C =

37429905404501534607575032853061861919929056665742172897475
39514996004934033287513645492486337633774301286255575334966
37181719906318334226830429488947587362947572899528676633741
84229491285358626065584752140805895469469045852316765914506
85148847567050918500696504729656038960828441398089261129665
67003511295835248721385278525507963863591668536984656542458
43169317558400096420522663381297134068766085988278028981523
41049257474155512683950212247141008561950455060178732845374
35867788066502671794887477630414229934189148251245909551866
02635772889546431086323955192428379633482311947255066505198
20637684693550668324588185

DOSSIER n°454-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 =

13004972385751219837882489639719010863773730188962420364409
29923391050536240426128591540489629419294442013533425912153
80613166209987481884804232055349228047579908782602558147154
08122951870784107251891616119911476380259735785612428980183
10810939064921816855228100770285229056602140833006644266008
96560865052474136424444046457274299087437149359288187598271
72442571533356366969920566508328163575813139227105998747765
12438702095162313655492543769812341312618879584008498131732
18266701830018919251438370862072824736313097372640650472503
85472605769686443656890592243349743039921410490666112908696
735278828570731050299515967

DOSSIER n°454-C :

Document ultraconfidentiel de la direction ennemie :

Chef, il me semble qu'il y ait eu une fuite parmi nos communications suite à la capture de deux de nos agents car, malgré notre changement récent de procédure de sécurité, certains cryptanalystes du groupe CA ont semble-t-il trouvé certains de nos codes secrets. Par mesure de sécurité, j'ai donc immédiatement changé notre clé e avec un générateur qui ne souffre d'aucune faille pour être définitivement à l'abri de toute attaque cryptographique et communiquer en toute sécurité.

DOSSIER n°454-D :

Note du service du chiffre de l'état-major

Après une étude approfondie du système, ce message semble similaire à celui du [dossier n°448](#). Néanmoins, 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) et les générateurs des paramètres utilisés ne semblent souffrir d'aucune faille, donc le déchiffrement paraît absolument impossible !