Du RSA sécurisé ?

Cette énigme a été créée par **jaudi**

Votre état-major a intercepté des documents confidentiels récupérés sur un espion ennemi et vous les a confiés pour que vous essayez d'en décrypter le contenu :

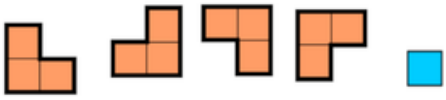
DOSSIER n°448-A :
Message chiffré envoyé par l'espion et intercepté par nos agents :
C =
338789592373475127556038191056753088048244593856299853194217207443071462357334110499932233486245815673145691927603316852588310254301943087125365137660562952193307257725039978700619487326261246429827021549975267074615127335177250399587997046399934409430686531511176631447367817567863963662254015908661729135610797328746863477538220655072227414256381944397935474586724578628103891679298767409501093104840252754509721561396504039165032787890704041700371584969686058378654102795330595270323252398624670640698624531459357987706149097667260617646908941063884105574795492839705113626141498494152255112314784527046885195770

DOSSIER n°448-B :

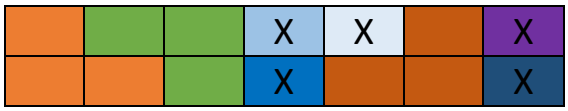
Cours de dénombrement – Exercice :

Quel est le nombre possible de pavages permettant de remplir un damier de 2 x n en utilisant seulement deux polynomios : un domino 1 x 1 et un autre en forme de L correspondant à un domino 2 x 2 auquel on a enlevé un coin ?

Les dominos peuvent être mis dans n'importe quel sens pour remplir le damier mais toutes les cases doivent être remplies pour valider le pavage. Exprimer le résultat sous une forme explicite f(n) pour tout n entier naturel.



Exemple de pavage 2 x 7 (avec trois L en orange, vert et orange foncé et 5 dominos 1 x 1 marqués par un X en nuances de bleu et de violet) :



DOSSIER n°448-C :

Fonctionnement du chiffrement RSA (notes inspirées du cours « Initiation à la cryptographie » sur Club Alkindi, fiche n°7, rédigée par Saint Erulo)

Le modulo (qui correspond au reste de la division euclidienne de deux entiers) est une opération très utilisée en cryptographie, notamment dans le chiffrement inventé par Rivest, Shamir et Adleman.

Pour le chiffrement RSA, Alice va choisir deux grands nombres premiers p et q pour calculer N = p x q puis phi(N) = (p-1)(q-1), ainsi qu'un autre entier e qui vérifie : PGCD(e, phi(N)) = 1.

Avec sa clé publique (N, e), Alice va ensuite calculer sa clé privée d vérifiant : $e*d \equiv 1 \bmod phi(N)$

Par la suite, son ami Bob pourra lui envoyer un message chiffré C, qui utilise la clé publique (N, e) publiée par Alice et est obtenu à partir du message clair B avec la formule : $C = B^e \bmod N$.

Seule Alice, qui connaît les entiers p et q et donc sa clé privée d, va pouvoir déchiffrer le message de Bob via la formule :
$C^d \equiv B^{de} \equiv B^{phi(N)*k+1} \equiv B \times B^{phi(N)*k} \equiv B \times 1^k \equiv B \bmod N$.
Une espionne comme Eve, qui surveillerait les communications entre Alice et Bob et qui aurait la clé publique (N, e) ainsi que le message chiffré C, ne parviendrait pas à le décrypter si N est suffisamment grand, notamment grâce au fait que, pour des grands nombres, il est extrêmement compliqué (voire impossible) de trouver leur décomposition en facteurs premiers si elle est composée de deux facteurs premiers très grands.

DOSSIER n°448-D :
Clé publique (N,e) de l'espion trouvée dans les bases de données :
N =
14674586647926905537460474990991631393939381731521675145002
13955281521957860680280727386216576518670419053410494192379
90105388478752350019398907335368739035035924346527603331129
66520390642945627286946447077269288880493088504290500467678
95048335694348755012442849553005837433500841153862263102138
37101321456876225152821553295484370994445428304843377412363
48001514534690633914365340097808081324812275323596740939092
56624470763924153794948949747345876396280069552968908882030
25078246236095695410849201940091631529793266409199704969618
18466510409336299486890331344464195193034720994485649083664
92364043834886620352902280 9

e =
94258964592596882943617720109141164975944700319717639440957
84310652155408210753913501921942677362461850869036147736837
91678425472378221430349179090387301518408927208067513554362
78093744383022377925395343156943133210463015297699229083746
35177128819797723777777080745052281327803558858282178277891
83628461592852780075991507438775687310011686229926021915849
47461649624065093918830969724982907397184268970001386355525
19882064563012602670755214981989767942915455208725300165542
63680940500426626638387263373674625990910340686984174758024
09316898651192233503226336004296622201199123286726922499410
59270393211551415888417221

DOSSIER n°448-E :

Note du service du chiffre de l'état-major

Après une étude succincte du système, il semblerait qu'il s'agisse d'une sorte de chiffrement RSA avec une clé publique N très grande (d'environ 2048 bits, ce qui correspond au standard de sécurité actuelle pour les banques et les gouvernements) donc le déchiffrage semble impossible… sauf si la génération des nombres présente une faille !

DOSSIER n°448-F – AJOUT RECENT AU DOSSIER :

Bout de papier chiffonné retrouvé dans les vêtements de l'espion :