07 /06/2013

CRAKAGE DU SYSTEME DE CODAGE RSA

selon les fait nous somme dans la période des guerres de gog&magog donc il faut enqueter au niveau de l'information (voir se que cache la grande prostituer ---> Babylone) et pour ça il faut factoriser le produit de facteur premier N=P_1P_2 a la base du systeme de codage rsa.

(principe du systeme rsa ----> http://www.cryptage.org/rsa.html).

copie du 15/05/2013 pour la 1er stratégie

Comme vous savez surement se systeme est celui utiliser pour cripter toutes les informations importante (transaction financière , infos privé et autres) donc celui qui arrive a casser le produit P_1P_2 peut voir toute les preuves de complot quelconque... hhh tout se que vous savez pas vous le trouverez probablement par le calcul.

Voila mon idée de base pour se programme de recherche que vous allez mettre au point si vous avez rien de plus éficace (niveau scolaire minimal des membres : 1er ou terminal voir moins)

2 stratégie

La première stratégie est de ramener le problème arithmetique à un probleme élémentaire de géométrie (simple étude de figure géometrique traiter par ordinateur avec une puissance de calculs multiplier en méttant en série tout les ordinateur des membres du collectif de recherche en utilisant par exemple un logiciel comme celui la :

http://www.astrocaw.eu/2011/05/le-calcul-partage-en-astronomie-sous-boinc/

dabord on peut chercher une courbe d'équation y=f(x) lier au nombre N=AB avec A et B premier et sur laquel on va relier des points qui vont former la figure géométrique a étudier dans le sens des invariant et relation par rapport à elle méme en remplaçant le produit de facteur premier AB par un autre produit de facteur P_1P_2 etc...

J'ai pensé que le mieux c'est que sa soit une courbe polynomiale de façon a avoir le maximum d'outil (un peut d'algébre pour aider) donc le plus simple c'est d'écrire le systeme de 2 équations:

S ---> Ln(A)+Ln(B)=X & Ln(A)Ln(B)=Y

se qui donne la fonction polynomiale : $Y= -x^2+Ln(AB)x$ (ne pas confondre grand X et petit x) . c'est donc une parabole et on peut d'entrer de jeux voir une des figures géométrique quil faudra entrer dans le programme de calcul c'est a dire le triangle de sommet [0,0] , $[Ln(AB)/2,(1/4)Ln(AB)^2]$ et le sommet normalement inconnue [x,Y].

Vous pouvez commencez par faire le programme informatique de recherche des propriétés commune dans un ensemble d'échantillon de nombre N=AB (on peut surement limitter la recherche en testant un millier de nombres sa devrai sufir ...je sait pas trop) que l'on peut classer au tout début avec le nombre de chiffres de chaque facteur premier et généré aussi d'autre produit AB à tester en permutant indépendemant les chiffres dans les deux facteur etc...(un peu de théorie des groupes).

bon ok, alors au moins 2 type de travaux:

1/ le programme informatique doit pouvoir étudier chaque figure géométrique et trouver lui méme les relation particulière (il faut un programme qui doit doit pouvoir etre enrichie au fil du temp par les membres) .

2/ chaque membre du projet doit pouvoir proposer (si il veut) une nouvelle classe de figure géométrique qui sera alors rajouter dans l'ensemble des figure géométrique étudier par le programme informatique (aprés vérification bien sur) et doit aussi pouvoir demander qu'une certaine propriété (quil trouve lui méme) soit tester par le programme (a la condition que se soit une propriété indépendante des autres bien sur) etc... voyez le truc ? chaqu'un peut rajouter ses trucs directement ou en envoyant a l'administrateur (je sait pas comment on l'appel) .

je donne un autre exemple de triangle (pas besoin de vous dire de vérifier tout les calculs ok et sqrt=racine carré) :

1/ f'(x_0)=0
2/ f(x_0)= (1/4)Ln(AB)²=Y_0
3/ x²-Ln(AB)x+Y=0 , x= (1/2)[Ln(AB)+ou-sqrt(Ln(AB)²-4Y)]
4/ je met en relation la parabole y=f(x) avec sa parabole symétrique (tangente nul au point [x_0,-Ln(AB)²] c'est à dire la parabole d'équation x²-Ln(AB)x=Y_2) en remplacant Y par Y_2=-Ln(AB)² dans la formule de résolution.
5/ sa donne x' = (1/2)[Ln(AB)+ou-sqrt(2Ln(AB)²)]=[[1+ou-sqrt(2)]/2][Ln(AB).
6/ je calcul la valeur de f(x')= [5/4+ou-sqrt(2)][Ln(AB)²]= Ln(A')Ln(B')=Y' avec A' et B' apriori réel .

ici on a déja un couple de sommet possible (0,0) , (x',Y') et le sommet normalement inconue (x,Y). etc...c'est à dire qu'à la limitte on peut par exemple remplacer Y dans la formule de résolution x= (1/2)[Ln(AB)+ou-sqrt(Ln(AB)²-4Y)] par n'importe quel valeur d'une fonction Y' associer à un certain raisonement pour avoir le point [x',f(x')]

---

on peut aussi éssayer d'étudier l'imbrication des 2 systeme (sa fait une recherche de relation algébrique et sa donne des points du plan pour faire des triangle ou autre :

S_1 ---> Ln(AB)=X & Ln(A)Ln(B)=Y
S_2 ---> Ln(A'B')=X' & Ln(A')Ln(B')=Y'

exemple : puisque les systemes sont identique on peut permuter les couples A,B et A',B' dans la valeur de f(x') se qui donne Ln(A)Ln(B)=-[5/4+ou-sqrt(2)]Ln(A'B')² .

---

on peut étudier les solution du systeme

S_3 ---> Ln(A")+Ln(b")=Ln(AB) & Ln(A")Ln(B")=-[5/4+ou-sqrt(2)]Ln(AB)²]
qui est quelque part en relation avec les 2 système
(trouver Ln(A'B') c'est équivalent à trouver Ln(A)Ln(B))

Remarque: si quelqu'un vous dit que tout ça c'est déja fait et quil ny a rien il faut leur demander les résultat de tout ça (tout le dévellopement de la stratégie) .en effet mes ptits amis , si les nombres cache des relations alors la géométrie+l'algébre linéaire+l'analyse+un peut d'arihtmetique qui permettent de dévelloper cette stratégie économique ne peuvent probablement pas passer à coté.

Propriété de la courbe d'équation : f(x)= -x²+Ln(P_1P_2)x=Y

Si la dérivé f'(x) donne la valeur Ln(P_1)Ln(P_2)=Y en x alors on a : 4f(x)=(X+Y)(X-Y) c'est a dire

que f(x) est solution de l'équation différentiel : $4Y+(Y')^2=X^2$
c'est un triangle rectangle de coté {2 sqrt(Y) ,Y' et X } .
(2 carré parfait c'est pas une convention)

1/ résoudre l'équation différentiel .
2/ chercher les conditions initial .
3/ exploiter l'invariant géométrique pour trouver d'autre invariant ou relations et critére de façon a réduire une certaine zone de probablilité dans laquelle se trouve la valeur inconnue.

---

remarque :
concernant le systeme de criptage RSA c'est relativement le plus sur http://villemin.gerard.free.fr/Crypto/RSA.htm (théoriquement sur à 100% par rapport aux moyens connu et en pratique sur à ~ 99,8 % http://www.maxisciences.com/rsa/rsa-le-systeme-de-cryptage-le-plus-securise-a-un-defaut_art21831.html) __ tout les complot et réseaux de l'axe du mal se cache dans se systeme de codage donc on peut me poser la question trés simple : faisons l'hypothèse que se systeme de codage peut etre casser géométriquement etc... pourquoi tu met public ? et bien tout simplement parceque le résultat est le méme ! si les complotiste malsaint trouve les premier ils changerons de systeme de codage mais le probleme c'est que rien est sur en dehors du RSA donc les informations serons quand méme visible par le coté positif de la force hh voila donc relax , (le léviatan fuyant) __

2ieme stratégie

2ieme stratégie ---> clef secrete de Fabricio Végass---> utiliser une 5 ieme opération élémentaire ---> * ----> (x*y)=x&y, exemple (3*5)=35 ----> vers recherche de relations clef, exemple ---------> **$(x*y)^2=x^2*y^2+[2(10)^k](xy)$** _avec k=nombre de chiffre de y_ {pour que cette relation fonctionne, il faut completer y^2 avec des 0 vers l'intérieur de la composition x^2*y^2 tel que le nombre de chiffre soit identique à $(x*y)^2$}. exemple : $(37*2)^2=1369*04+20(37)(2)=(372)^2$. vous poser y=1 et vous déduisez des règles de calcul etc...c'est une clef pour la recherche par l'arithmétique modulaire qui est aussi lier indirectement aux forme modulaire a l'aide d'aplication sur les deux membre de certaine relation contenant +,X et * qui permettent de faire des tables d'opération .(des invariants). exemple ---> §(x*y)=§(x+y) ou § est l'application qui fait la somme des chiffres jusquau chiffre de base { 1,2,3,4,5,6,7,8,ou 9}__Fabrice B

Voila les grandes ligne des idées que j'avait pensé il y a plus de 10 ans à temp "perdu" mais comme j'était seul je ne me souvient plus très bien se que j'avait commencer a faire ni ou je me suis arréter mais je vais donner les bases et vous trouverez se quil faut faire pour réussir si c'est une bonne direction.

La stratégie est simple et elle est fondé sur l'introduction d'une opération d'assemblage en série *

N=P_1P_2

1/ calculer le nombre d'ocurence des chiffres qui compose les facteur P_1 ou P_2
2/ trouver la permutation qui forme le nombre P_1 ou P_2 par rappor a la permutation qui donne le l'entier N à partir d'une configuration initial pris comme permutation identité. (ordonner du plus

petit au plus grand par exemple : (a_1)*a_2*.....*a_k avec a_i<a_i+1)

exemple : N=1465

Je par de l'idée d'obtenir le chiffre N par une combinaison linéaire en introduisant une opération d'assemblage en série * qui consiste simplement a mettre 2 chiffre cote a cote pour avoir un nouveau chiffre . a*b=a&b . exemple ---> 10*1=101.

ensuitte je pose l'hypothèse quil existe une relation entre les 2 permutations des facteurs P_1 et P_2 et la permutation qui donne
N ---->N= σ [k_1•(0)*k_1•(1)*k_2•(2)*.....*k_n•(n)] =P_1P_2
avec le produit • par les scalaire entier ---> k•a=(a)*(a)*...*(a)=aaaaaa...aa = k fois ok.

---

voilà les éléments de base pour appliquer la stratégie :

1/ les entiers de la base 10 {0,1,2,3,4,5,6,7,8,9}.

2/ l'opération élémentaire *.

3/ les ensembles de permutation muni du produit classique ° et de l'opération * .

4/ des tables de calcul par une aplication de fabrice (on va l'apeler l'aplication § c'est une application qui permet de faire des tables d'opération ,exemple --> §(x*y)=§(x+y) ou § est l'application qui fait la somme des chifres jusquau chiffre de base {1,2,3,4,5,6,7,8,ou 9}.

5/ un théorème de fabrice sur les ensembles de permutation {S_i} muni de ° et *(que j'ai perdu mais c'est pas grave vous le retrouverez nécéssairement.

6/ (élément en plus que j'ai trouver en 2013) → généraliser un algoritme de multiplication

---

1er étape :

1/ ----> <u>convention d'écriture des permutions pour le calcul pratique .</u>

**Pour pouvoir vérifier des choses il faut avoir un moyen de calcul pratique mais dans la convention d'écriture que l'on trouve dans les manuel de mathématiques n'est pas adapter donc Je commence par considéré les permutations comme des vecteur de R^n et je pose la permutation de gauche comme étant un opérateur qui agi sur la permutation de droitte.
Exemple : X°Y=(1,3,2)°(2,3,1)=(2,1,3) c'est a dire que les composantes de l'opérateur indique la case de la permutation qui va prendre la place sa place c'est a dire si x et y sont deux permutation de S_n alors on a x°y=y_x.**

**Dans l'exemple la composante n°1=1 de l'opérateur X indique que la composante n°1 de la permutation Y va passer dans sa case n°1 .
La composante n°2=3 de l'opérateur X indique que la composante n°3 de la permutation Y doit passer dans sa case n°2.
La composante n°3=2 de l'opérateur X indique que la composante n°2 de la permutation Y doit passer dans la case n°3.**

Avec ma combine les calculs se font rapidement exemple :
(2,6,1,7,4,5,3)°(2,6,7,3,1,4,5)=(6,4,2,5,3,1,7)

2/ ----> <u>facilité le produit des permutation , ordonner les permutation a partir de l'indentité selon une convention aproprier</u>

voila ma méthode :
j'écrit une permutation en entier et j'ordonne de gauche a droitte .
ex: S_3

(1,2,3) ---> 1er permtation de S_3
(1,3,2) ---> 2ieme permutation de S_3
(2,1,3) ---> 3ieme permutation de S_3
(2,3,1) ---> 4ieme permutation de S_3
(3,1,2) ---> 5ieme permutation de S_3
(3,2,1) ---> 6ieme permutation de S_3

je fait le produit en utilisant la permution de gauche comme action sur celle de droitte et cette action est un opérateur (change une permutation de S_3 en une permutation de S_3) indiquer par les composante de la permutation :
exemple: (2,1,3) ---> (3,2,1) = (2,1,3)°(3,2,1)= (2,3,1) c'est a dire que la 1er composante de l'opérateur (2,1,3) indique la composante de la permutation qui doit passer en 1er place.
La 2ieme composante de l'opérateur indique la composante 3 de la permutation qui doit passer en 2ieme place et finalement la 3ieme composante de l'opérateur indique la composante 1 qui doit passer en 2ieme place . voila c'est simple et le produit se fait trés rapidement mais il faut écrire toute les composantes de la permutation .

2ieme exemple: (1,7,5,2,4,3,6)°(3,5,1,2,7,6,4)=(3,4,7,4,2,1,6) c'est assez rapide a faire alors que dans les manuel habituel toute les permution sont écrite sous une forme qui n'est pas adapter aux calculs pratique (qui sont nécéssaire pour vérifier des relations et nouveau théorème (les propriétés et autres) par rapport a l'opération * et ° sur tout les ensemble de permutation {S_i} i variant de 1 à l'infini ou de 0 à l'infini en rajoutant la permutation vide (je me rappel plus trés bien mais j'ai introduit cette permutation comme un moyen ou comme nécéssaire dans le but de définir la structure (à inventé ou alors existe déja comme un genre d'algebre non commutatif) c'est a dire l'élément O tel que O+x =x ou x est une permutation quelconque ,).
de façon formel le produit sécrit .....

<u>3/---> définir l'assemblage en série sur les permutation avec l'opération * .</u>

Bon , moi j'ai utiliser la relation d'ordre pour définir un premier assemblage avec * exemple:

(1,3,2)*(3,2,1)=(1,3,2,6,5,4) c.a.d que je considére la 2ieme permutation comme le complémentaire dans S_6 donc équivalente à la partie (6,5,4) de (1,3,2,6,5,4) soit (3,2,1)~(6,5,4) , bon évidément on a ---> (S_n)*(S_m) E S_(n+m) avec E=appartient.
j'introduit donc la permutation vide S_0=(0)=(rien) qui servira à définir la soustration (je me rappel plus mais je vais définir tout ça)

remarque :

c'est par rapport a cette opération d'assemblage en serie * que j'ai pensé à chercher à "factoriser" la permutation particulière connu a partir de P_1P_2 .
S_(i+j)=(S_i)*(S_j) . on voit déja que se sous ensemble de S_(n+m) muni du produit ° est un sous groupe .

vérifiant sur S_4
(appelons cette ensemble X)
(1,2)*(1,2)=(1,2,3,4)= p_(1,4)=permutation n°1 de S_4
(1,2)*(2,1)=(1,2,4,3)=P_(2,4)=permutation n°2 de S_4
(2,1)*(1,2)=(2,1,3,4)=P_(3,4)=permutation n°3 de S_4
(2,1)*(2,1)=(2,1,4,3)=P_(4,4)=permutation n°4 de S_4

voila et on peut vérifier que le produit de deux quelconque permutation de cette ensemble est encore une permutationde cette ensemble.
quelque exemple:
P_(1,4)°P_(1,4)=P_(1,4)
P_(2,4)°P_(1,4)=P(2,4)
P_(2,4)°P_(2,4)=P_(1,4)
P_(3,4)°P_(4,4)=P_(2,4)
etc...(j'ai vérifier ça il y a longtemp donc j'arrete à ses quelque exemple)

Bon pour la suitte je compléterez le pdf plus tard mais normalement vous savez se qu'il faut donc je passe a la 3ieme stratégie qui est en fait une composante de la 2ieme stratégie que j'ai trouver il y a quelques mois.

//

3ieme stratégie ---> Algoritme a généraliser (je l'ai trouver dans un jeux mathématique fait par des amateurs donc pas connue):

produit de 2 nombre entier inférieur à 20:

Exemple: 18 x 16 =288
Etape 1: Additionner le chiffre des unités du plus petit nombre avec le plus grand
6 + 18 = 24

Etape 2: Multiplier le resultat de l'étape 1 par 10
24 x 10 = 240

Etape 3: Multiplier les unités des deux nombres
8 x 6 = 48

Etape 4: Additionner 2 et 3 pour la reponse finale
240 + 48 = 288

Cette algorithme de multiplication est très intéréssant et utilise l'opération ''d'assemblage en série''* .

La première étape est donc de généraliser et voilà se que je trouve aprés une recherche ''hazardeuse'' (c'est bien le cas général ,en fait j'ai généraliser en dimmension inférieur ou égal a 2 et ensuitte il suffit de moduler) ----> X et Y inférieur ou égal a 2

X=a*b* , Y=c*d*

Si c<b ---> XY=(a*b)(c*d)=(10c)(a*b+d)+10(c-a)d+bd
Si c>b ---> XY=(10c)(a*b+d)-10(c-a)d+bd

pour généraliser il retse à ‘’moduler’’ (je considére que cette ‘’modulation’’ est une véritable opération élémentaire étant donner quelle m’a aussi servi pour résoudre les équations algébrique de degrés 1,2,3,et 4 par une méthode personnel plus belle que celle de lagrange). bon ok je pose (a*b)=A et (c*d)=B se qui donne : X=A*B et je met en facteur Y=[(e*f)*(g*h)]=C*D :

XY=[(a*b)*(c*d)][(e*f)*(g*h)]= (A*B)(C*D) et il reste à comprendre que la dimmenssion est divisible par 2 et quil faut élever le facteur 10 a la puissance N/2. Si a X ou Y est de dimmenssion 3 alors il suffit de remplacer a ou e par 0 etc...

sa donne : .

Si C>A ----> (A*B)(C*D)=[10^(n/2)+C](A*B+D)+(10^(n/2)(C-A)D+BD
Si C< A---> (A*B)(C*D)=[10^(n/2)+C](A*B+D)-(10^(n/2)(C-A)D+BD
n=dimension des facteurs ---> 2^k avec k=1,2,3,....,etc.

ensuitte il faut généraliser en dimmenssion 8 etc ...c’est a dire moduler la dimmenssion 2.

Bon voilà , la deuxieme étape est d’inversser l’algorithme ! Je vous laisse faire ok, allez salut et a la prochine mise a jour du pdf .

Fabrice f Brésil
==========
==========
==========