

Pratique de RSA

Malika More

`(malika.more@iut.u-clermont1.fr)`

IREM Clermont-Ferrand

Formation ISN

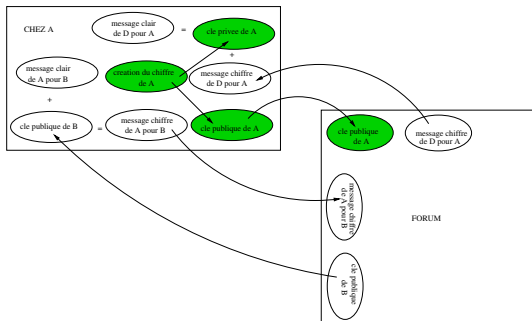
2011 - 2012

Dispositif de TP

- Avec Maple + ENT
- RSA (presque) en vrai grandeur
- Nombres premiers de 150 chiffres environ
- Factorisation impossible à notre niveau

Phase 1 : Création du chiffre

- Maple : Génération des clés privées et publiques
- ENT : Publication des clés publiques



Phase 1 : Création du chiffre

```

File Edit View Insert Format Tools Window Help
[Icons]
C Text Times New Roman 12 B I U [Icons]

Le nombre e ne doit plus changer jusqu'à la fin de ce TP, et pour s'en assurer, vous devez le copier-coller ci-dessous :

> e:=31940164296236785911957303597819558194397945141777287694718722890153188711113927909985234147
9339757;
e :=31940164296236785911957303597819558194397945141777287694718722890153188711113927909985234147933\
9757

Question 5 - Calculer le faciltieur correspondant au compliqueur e et ranger le résultat dans la variable d.

> d:=e^(-1) mod m;
d := 3776831173867858931896820804608267916128965884130544057338235750611058919357036732538381498516\
12293

Question 6 - Il ne vous reste plus qu'à publier la partie publique de votre code secret. Pour cela, vous devez simplement la poster sur le
forum de cryptographie de votre groupe de TP, sur le serveur web de l'IUT en ligne, auquel vous avez accès pendant cette séance de TP.
Attention toutefois à ne poster aucun élément de la partie privée de votre code !

Parmi ces éléments privés, il y en a que (dans la vraie vie, pas dans ce TP) vous feriez mieux de faire disparaître par sécurité, et d'autres que
vous devez absolument conserver en lieu sûr, lesquels ?

[Ready] [Time: 0.00s] [Memory: 0.18M]

```

IUT de Clermont - Ferrand

4 users connected

Accueil

 [Plate-forme Pédagogique](#) > [Codes et Cryptographie en semestres décalés](#) > [Groupes](#) > [Groupe 1](#) > [Forums](#)

Mode de navigation : **Classique** | Optimisée
Mode de vue : Étudiant | Gestionnaire de cours

► **Forums**

[Forum Index](#) > [Groupe 1](#) > **Boite aux lettres RSA Dumenil Mikotajewski**

Répondre | Rechercher

Boîte aux lettres RSA Dumenil Mikotajewski

☐ M'avertir par e-mail quand une réponse est postée

Initiateur : Maxime Mikotajewski Posté le : Mercredi 02 Juin 2010 à 16:24

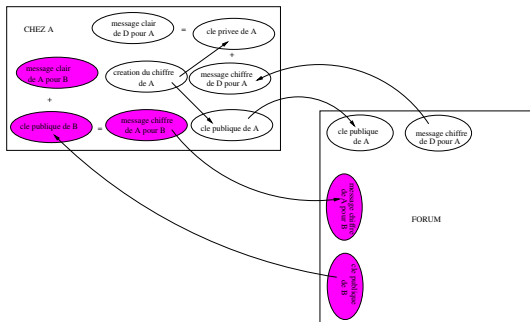
e : 104664352565476084770647085442386988012787864288360763336231408463390320223995829736268988686304664309

n: 180013984037039567164518161523998752282100198485434238061897089348183356404765823615641393415427851187

Initiateur : Yoan Poigneau Posté le : Mercredi 02 Juin 2010 à 16:38

Phase 2 : Chiffrement d'un message

- ENT : Récupération des clés publiques des destinataires
- Maple : Chiffrement des messages
- ENT : Publication des messages chiffrés



Phase 2 : Chiffrement d'un message

```

File Edit View Insert Format Tools Window Help
[Icons]
C Maple Input [Monospaced] [12] [B I U] [Align] [List] [Undo] [Redo]

Question 1 - Tapez votre texte ci-dessous. Votre message doit comporter au moins 3 lignes de texte.

> texte:= " Un systeme d'informations (si) est l'ensemble des informations (données), des
traitements, événements et résultats liés au fonctionnement d'une entreprise ou d'une
organisation. Le cours d'ACSI présente des méthodes pour étudier un système
concevoir une solution informatisée ou application qui réponde aux souhaits des usagers.";

|
texte := " Un systeme d'informations (si) est l'ensemble des informations (données), des traitements, événements et résultats liés
au fonctionnement d'une entreprise ou d'une organisation. Le cours d'ACSI présente des méthodes pour étudier un système
d'information et concevoir une solution informatisée ou application qui réponde aux souhaits des usagers."

Question 2 : Coller ci-dessous la clé publique de vos destinataires qui se trouve sur le forum (dans leur boîte aux lettres), et la ranger dans les
variables "Nbis" et "ebis".

> Nbis:=
78381831683756643872658540141444397676434491715759542266480222995746893292133963595646667500998
660088114535060531839451507672940153686096324832280671574541811082199;

Nbis := 78381831683756643872658540141444397676434491715759542266480222995746893292133963595646667500998660\
088114535060531839451507672940153686096324832280671574541811082199

> ebis:=77917451071264293268441155899465527701710461957381022421697306072282206924665538810956366
303008661300306643731635608057643635014336505043403300361345654405158830035

[Ready] [Time: 0.00s] [Memory: 0.18M]

```

Phase 2 : Chiffrement d'un message

```

File Edit View Insert Format Tools Window Help
[Icons]
C Text Times New Roman 12 B I U [Icons]

Question 5 : Convertir votre message texte en un message numérique en utilisant la fonction "encodenum". Ranger le résultat dans la
variable "messnum".

> messnum:=encodenum(longbloc, texte);

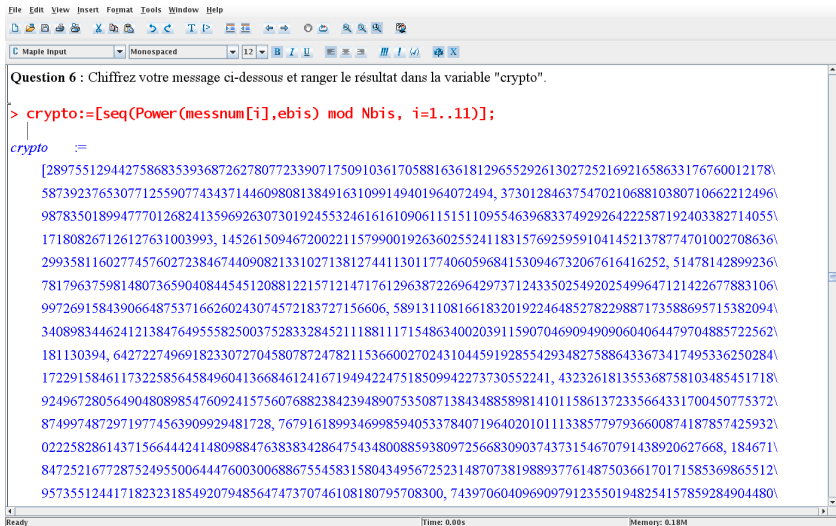
messnum :=
[32041105115040032115110111105116097109114111102110105039100032101109101116115121115032110085032,
21151101111051160971091141111021101050321151011000321011080981091011151101010391080321161151010,
23311823303204411511611010110910111610509711411603211510110003204404111510123311011011110004003,
10111102032117097032115233105108032115116097116108117115233114032116101032115116110101109101110,
2117111032101115105114112101114116110101032101110117039100032116110101109101110110111051160991,
3910003211511411711109903210107603204611011110511609711510511009710311411103210111011703910003,
3211411711112032115101100111104116233109032115101100032101116110101115233114112032073083067065,
1111051160971091141111021101050391000321011092331161151211150321101170321141011051001171162330,
11110211010503211011110511611710811111503210111011703211410511111810109911011109903211610103211,
11112233114032105117113032110111105116097099105108112112097032117111032101233115105116097109114,
461151141011030971151170321151011000321151161050971041171111150321201170970321011001101]

La commande ci-dessous compte le nombre de blocs de votre message numérique.
> nbrebloc:=nops(messnum);

```

Ready Time: 4.55s Memory: 4.99M

Phase 2 : Chiffrement d'un message



The screenshot shows the Maple software interface. The title bar includes 'File', 'Edit', 'View', 'Insert', 'Format', 'Tools', 'Window', and 'Help'. The menu bar contains icons for file operations, editing, and viewing. The toolbar shows various mathematical and editing tools. The main window displays the following text:

Question 6 : Chiffrez votre message ci-dessous et ranger le résultat dans la variable "crypto".

```
> crypto:=[seq(Power(messnum[i],ebis) mod Nbis, i=1..11)];
```

The variable `crypto` is assigned a long sequence of 11 numbers, each followed by a backslash character. The sequence is:

```
[28975512944275868353936872627807723390717509103617058816361812965529261302725216921658633176760012178\
587392376530771255907743437144609808138491631099149401964072494, 37301284637547021068810380710662212496\
987835018994777012682413596926307301924553246161610906115151109554639683374929264222587192403382714055\
171808267126127631003993, 14526150946720022115799001926360255241183157692595910414521378774701002708636\
299358116027745760272384674409082133102713812744113011774060596841530946732067616416252, 51478142899236\
781796375981480736590408445451208812215712147176129638722696429737124335025492025499647121422677883106\
997269158439066487537166260243074572183727156606, 58913110816618320192246485278229887173588695715382094\
34089834462412138476495558250037528332845211188111715486340020391159070469094909604064479704885722562\
181130394, 64272274969182330727045807872478211536600270243104459192855429348275886433673417495336250284\
17229158461173225856458496041366846124167194942247518509942273730552241, 432326181355368758103485451718\
924967280564904808985476092415756076882384239489075350871384348858981410115861372335664331700450775372\
87499748729719774563909929481728, 767916189934699859405337840719640201011133857797936600874187857425932\
02225828614371566444241480988476383834286475434800885938097256683090374373154670791438920627668, 184671\
847252167728752495500644476003006886755458315804349567252314870738198893776148750366170171585369865512\
95735512441718232318549207948564747370746108180795708300, 743970604096909791235501948254157859284904480\
```

The status bar at the bottom shows 'Ready', 'Time: 0.00s', and 'Memory: 0.18M'.

Phase 2 : Chiffrement d'un message

Boîte aux lettres RSA Dumenil Mikotajewski

 M'avertir par e-mail quand une réponse est postée

 Initiateur : Maxime Mikotajewski Posté le : Mercredi 02 Juin 2010 à 16:24

e : 104664352565476084770647085442386988012787864288360763336231408463390320223995829736268988686304664309

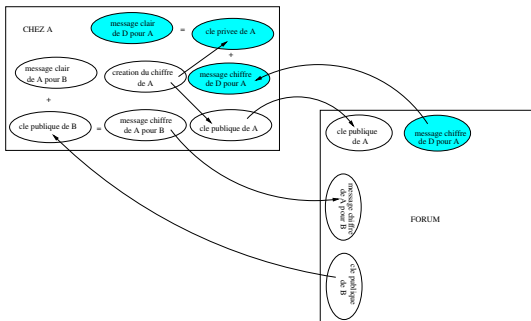
 n :
 180013984037039567164518161523998752282100198485434238061897089348183356404765823615641393415427851187

 Initiateur : Yoan Poigneau Posté le : Mercredi 02 Juin 2010 à 16:38

crypto :=
 [17752240210174621439201400764101012703222647172557303390263893085018789556504111155726693021343840123,
 14641944816361732155136938760408306677940583858527800546690907889113851060266661224171952522087649447,
 56087420428964678867002406580518043411400902877344419758507312717005637842744463030508177457873691195,
 62180632081408644539395265945303138010209270273092724569575571383991817896193951779797223789869548646,
 571648571203937709784763803284736333804438276495395959518840956922360078456437873450818831571852514,
 73323603058248003795152392514177657985897402837312592623984161450386242895321988509050838694259129218,
 59285237782926075244198824250068514833583184176558125804531913609959560287514528733114049385256939284,
 92031049270349306479124686031927855026530612855726500247927247689366614113654560973091674823663491378,
 8599901450168255359342357790501225916068512401819740765896897711057195398063302435236570496472213346,
 41767307886546643932552799524455679065217931525018459911750972005148488705025220489058050264896780493,
 60882809222302288739072522175831088459936687951553303792729579849551969786102795750921416441044318348,
 98653913162018780923012024620434532524514128923057298660845977073932559283689734250664446472607994111,
 52909958396728086746535266749986273741223735621581728402224564216031264434184768043175266432433711748,
 30890125586892775586332249365538548532788805981655513043526067781344848962059773977985784319047990038,
 136848963873300355229868097494714012359789788129441781265622725100934110435356115632990354613602096596,
 8399854844607430469686036941400914179012114437649738095926482560701697881076331328554770905445670445,
 70089903690492386395526130222084162239786992976956363169585498565542762871838163590582489293551773352]

Phase 3 : Déchiffrement d'un message

- ENT : Récupération par les destinataires des messages chiffrés
- Maple : Déchiffrement des messages chiffrés



Phase 3 : Déchiffrement d'un message

```

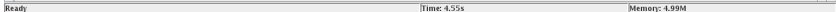
File Edit View Insert Format Tools Window Help
[Icons]
C Text Times New Roman 12 B I U [Icons]
Question 1 : Récupérer sur le forum le cryptogramme qui vous est destiné, et le ranger dans la variable "cryptobis".

> cryptobis :=
[3478278245556051587937723444558974030695949341786842737004118979755837384645403559534441112997
93130944990262239736301680302267049552357724475849542768310513,
17442741055819670626857562661395675169733499068870929996696281906723215484782263717668813178914
0838583504102099258399475253263057290339680841111342543325132,
31572827464694521325758429769243343110190083453435737404355971628031161366378594553122975760478
3103538121154668243160779364124832817087484159372371752538081,
20723038960052603002834916886737367750920946697800755088246880126787585787146039191326807756398
0008068727566847910833441507024394519224080221760968772034160,
31029534333419300665023185507300458462372314513352844902648906262006589100988685296252393781204
4475455773135477012423247898239144849635992210872196675854728,
38833274854941138687422788048296353238942675405531606495464576528647496762985530805367443182646
3442468422281602390247266765429546985699314961710703236077161,
36932093103321224902705382059657265295270791763340972100438670795772910190703392030494338863134
0378562022971849701173870290834634699302516269692186256717738,
34989682494117897766164539256276225226265645338778240326956094490462351169362064950010413517535
1966868476364835807040797103956159735377077178095464938500047,
33134190410769654222030596928142859031471183171677375697883938193832395616542507203471400511204
0385408255815431145292245016636478269926446291140315207734624];

cryptobis :=
[34782782455560515879377234445589740306959493417868427370041189797558373846454035595344411129979313094]

```

Ready Time: 4.55s Memory: 4.99M



Phase 3 : Déchiffrement d'un message

```

File Edit View Insert Format Tools Window Help
[Icons]
C Text Times New Roman 12 B I U [Icons]
La fonction decodenum prend en entrée un message numérique m et renvoie le texte qu'il représente (voir TP1).

> decodenum:=proc(m)
  local nbb1bis,lgb1bis,nbbis,nbchbis,nbcarbis,listearsciibis,i;
  nbb1bis:=nops(m);
  lgb1bis:=max(seq(length(m[i]),i=1..nbb1bis));
  nbbis:=add(m[i]*10^(lgb1bis*(i-1)),i=1..nbb1bis);
  nbchbis:=length(nbbis);
  nbcarbis:=ceil(nbchbis/3);
  listearsciibis:=[seq(irem(iquo(nbbis,10^(3*(i-1))),10^(3)),i=1..nbcarbis)];
  return(convert(listearsciibis,bytes));
end proc;

> decodenum(decrypto);

"dans la jungle, terrible jungle, le lion est mort ce soir! hoooo hi, ozinabouéé. Bien le bonsoir la jeunesse! Je voulais vous informer
qu'un membre de votre équipe était blonde ! Je compatie avec vous => frappe mi et frappe moi sont dans un bateau, frappe mi
tombe à l'eau, qui c'est qui reste??????? Mouahahahahahahahaha"

Partie 3 - Décrypter un code RSA.

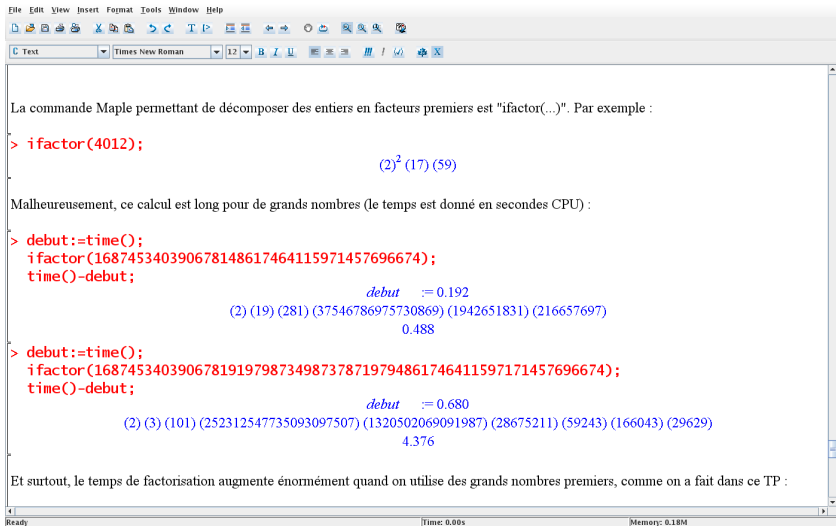
On se place dans la position d'un espion qui veut décrypter un cryptogramme qu'il a intercepté. S'il ne connaît que la partie publique du code
RSA, il lui faut arriver à calculer le facilitateur d à partir du module n et du compliqueur e. C'est-à-dire qu'il faut factoriser n pour retrouver p et
q, puis calculer  $m=(p-1)*(q-1)$  et enfin inverser e modulo m. En pratique, seule la première étape est difficile, car très longue, même avec les

```

Tests de sécurité

- Maple : Mesure du temps nécessaire à la factorisation de grands nombres

Tests de sécurité



```

File Edit View Insert Format Tools Window Help
[Toolbar icons]
C Text Times New Roman 12 B I U [Formatting icons]

La commande Maple permettant de décomposer des entiers en facteurs premiers est "ifactor(...)". Par exemple :

> ifactor(4012);

               (2)2 (17) (59)

Malheureusement, ce calcul est long pour de grands nombres (le temps est donné en secondes CPU) :

> debut:=time();
  ifactor(168745340390678148617464115971457696674);
  time()-debut;

               debut      := 0.192
               (2) (19) (281) (37546786975730869) (1942651831) (216657697)
               0.488

> debut:=time();
  ifactor(1687453403906781919798734987378719794861746411597171457696674);
  time()-debut;

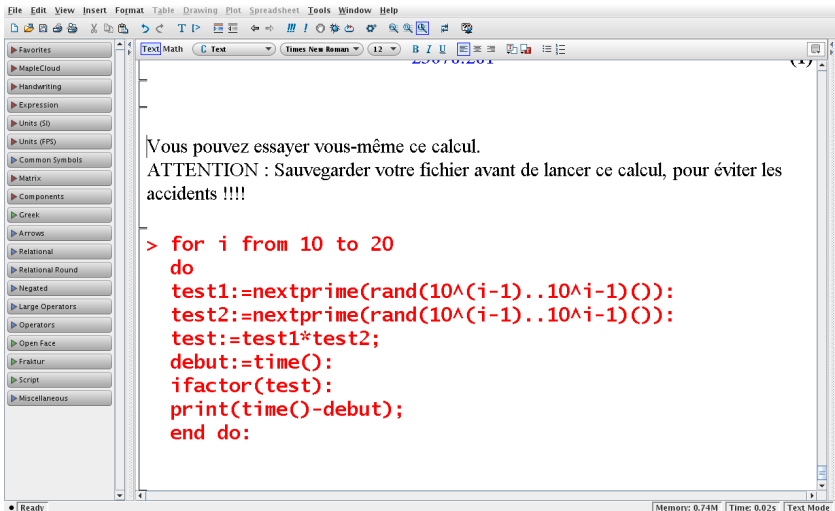
               debut      := 0.680
               (2) (3) (101) (252312547735093097507) (1320502069091987) (28675211) (59243) (166043) (29629)
               4.376

Et surtout, le temps de factorisation augmente énormément quand on utilise des grands nombres premiers, comme on a fait dans ce TP :

```

Ready Time: 0.00s Memory: 0.18M

Tests de sécurité



The screenshot shows a Maple software window with a menu bar (File, Edit, View, Insert, Format, Table, Drawing, Plot, Spreadsheet, Tools, Window, Help) and a toolbar. On the left is a sidebar with various tool categories like Favorites, MapleCloud, Handwriting, Expression, Units, Common Symbols, Matrix, Components, Greek, Arrows, Relational, Relational Round, Negated, Large Operators, Operators, Open Face, Fraktur, Script, and Miscellaneous. The main workspace contains the following text:

Vous pouvez essayer vous-même ce calcul.
ATTENTION : Sauvegarder votre fichier avant de lancer ce calcul, pour éviter les accidents !!!!

```
> for i from 10 to 20
do
test1:=nextprime(rand(10^(i-1)..10^i-1)):
test2:=nextprime(rand(10^(i-1)..10^i-1)):
test:=test1*test2;
debut:=time():
ifactor(test):
print(time()-debut);
end do;
```

The status bar at the bottom indicates: Ready | Memory: 0.74M | Time: 0.02s | Text Mode.

FIN