

# Travail Pratique : RSA

---

Cours : ISC\_121 - 2021-2022

Groupe 13 : Gawen ACKERMANN, Florian BURGNER, Quentin FASLER, Dario GENGA

## Introduction

---

La cryptographie existe depuis l'antiquité et est utilisée pour transmettre des messages de manière sécurisée. L'utilisation de la cryptographie a fortement augmenté avec la Première et Seconde Guerre mondiale où la confidentialité des transmissions était primordiale. De nos jours, nous l'utilisons quotidiennement sans forcément le savoir.

Apparu en 1977, le RSA porte le nom de ses auteurs :

- Ronald **R**ivest
- Adi **S**hamir
- Leonard **A**dleman

et sert à chiffrer des données de manière asymétrique, le RSA à cet effet utilise une clé publique ainsi qu'une clé privée.

Afin de déchiffrer le message que nous avons intercepté, nous allons utiliser divers outils mathématiques qui, utilisés ensemble permettent de lire le message en clair. Dans la suite de ce rapport, nous allons approfondir ces outils mathématiques en expliquant leur principe ainsi que leurs applications et comment ils nous ont permis de trouver le message ci-dessous.

***De toutes façons, les réunions de la Table Ronde c'est deux fois par mois. Donc, si le mec il dit après-demain à partir de dans deux jours, suivant s'il le dit à la fin du mois, ça reporte.***

(Sans doute une missive provenant de l'île de Logres, Kaamelott ?)

## Méthodologie

---

Dans cette partie du rapport, nous allons tout d'abord détailler les outils mathématiques nécessaires pour comprendre la méthode que nous avons utilisée pour casser le chiffrement, puis nous décrirons comment nous avons cassé celui-ci.

Pour rappel, ci-dessous, se trouvent les données que nous avons interceptées. Ces données ont été chiffrées avec le chiffrement *RSA*. Les variables  $n$  et  $e$  correspondent à la clé publique (nous reviendrons plus tard sur cette notion dans la suite du rapport) et la variable *encrypted\_data* correspond aux données chiffrées qui une fois déchiffrées et regroupées reconstituent le message que nous cherchons.

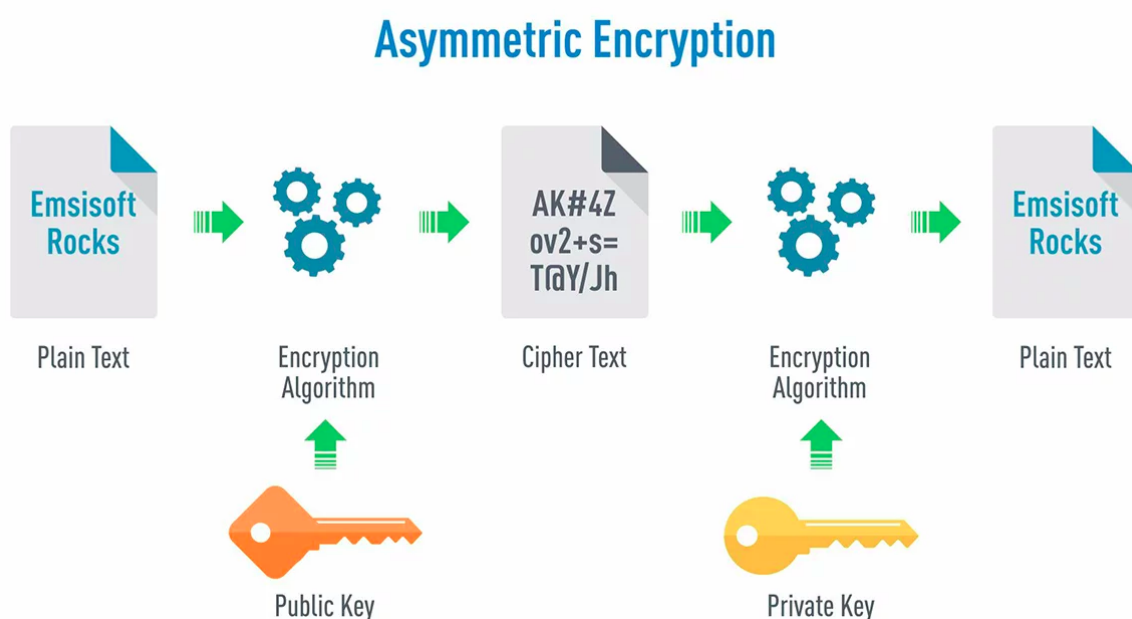
Variable	Valeur
n	1653973759
e	5249
encrypted_data	1511395078, 260436590, 1630654276, 1190458520, 790492067, 515550941, 297140366, 755589582, 647075331, 1191707844, 901889430, 660956124, 1500654109, 984322720, 1275630738, 1244853107, 1445928913, 1312523810, 265093060, 933013993, 1375592761, 195866064, 534502441, 928270408, 166404031, 621272622, 1304987439, 905393335, 55120151, 772595721, 506609577, 1172751778, 162439707, 233959833, 1468937795, 1358701120, 901889430, 495995733, 1524090698, 1043509086, 934992314, 1545639379, 1061595897, 1348452679, 1135067876, 905393335, 621272622, 55120151, 233959833, 1220119699, 708711266, 517797467, 195866064, 1579814353, 412378626, 498875436, 445485200, 7656659

## Outils mathématiques

Nous avons dû utiliser divers outils mathématiques afin de pouvoir déchiffrer le message intercepté, ces outils sont : le théorème de Bachet-Bézout, le théorème de Bézout, l'inverse modulaire, l'exponentiation modulaire et le principe du chiffrement RSA.

### Brève explication du RSA

RSA est un chiffrement asymétrique, il existe donc toujours deux clés, la première clé est la clé dite publique (utilisée pour le chiffrement) et la deuxième est la clé dite privée (utilisée pour le déchiffrement). L'image ci-dessous décrit le chiffrement et le déchiffrement de données asymétriques. Le "Cipher Text" correspond aux données "encrypted\_data" que nous avons interceptées.



Explication du chiffrement asymétrique

## Théorème de Bachet-Bézout et théorème de Bézout

Le théorème de Bachet-Bézout nous dit que le PGCD (**P**lus **G**rand **C**ommun **D**iviseur) de deux entiers relatifs  $a$  et  $b$  implique l'existence de deux entiers relatifs  $x$  et  $y$  tels que :

$$\text{PGCD}(a, b) = ax + by$$

Ce qui nous intéresse dans cette égalité sont les coefficients  $x$  et  $y$  qui nous seront utiles pour déterminer l'inverse modulaire d'un nombre que nous expliquerons juste après, mais avant cela il y a une autre notion importante à savoir : *le théorème de Bézout*.

Le théorème de Bézout nous dit que deux entiers relatifs  $a$  et  $b$  sont premiers entre eux (si et seulement s'il existe deux entiers relatifs  $x$  et  $y$  tels :

$$ax + by = 1$$

On peut donc en déduire que si le PGCD de deux entiers relatifs  $a$  et  $b$  est égal à 1 alors  $a$  et  $b$  sont premiers entre eux, encore une fois cette notion nous est utile pour le calcul de l'inverse modulaire.

## Inverse modulaire

L'inverse modulaire est une notion qui nous sert à calculer la clé privée du chiffrement RSA que nous utiliserons par la suite. Définition : l'inverse modulaire d'un entier relatif  $a$  dans les modulo  $n$  est un entier  $u$  satisfaisant l'équation suivante :

$$au \equiv 1 \pmod{n}$$

L'inverse modulaire pour un entier relatif  $a$  dans les modulo  $n$  existe seulement quand  $\text{PGCD}(a, n) = 1$ , autrement dit  $a$  et  $n$  doivent être premiers entre eux.

On peut donc calculer l'inverse modulaire avec :

$$1 = \text{PGCD}(a, n) = au + ny \quad (\text{théorème de Bachet-Bézout})$$

$u$  est l'inverse modulaire de  $a$  dans les modulo  $n$

## Exponentiation modulaire

L'exponentiation modulaire nous sert pour effectuer les calculs de déchiffrement. Nous allons expliquer l'exponentiation modulaire au travers d'un exemple, car cela est plus efficace pour comprendre l'algorithme. Nous voulons effectuer le calcul suivant :

$$14^{108} \pmod{22}$$

Comme vous vous en doutez, effectuer un tel calcul sur ordinateur est très lent, l'algorithme d'exponentiation modulaire règle ce problème. Afin de calculer le résultat, nous avons besoin de décomposer notre calcul en trois éléments : la base (14 pour notre exemple), l'exposant (108) et le modulo (22).

La **première étape** consiste à décomposer l'exposant en puissance de 2.

$$2^6 + 2^5 + 2^3 + 2^2 = 64 + 32 + 8 + 4 = 108$$

$$14^{64} * 14^{32} * 14^8 * 14^4 = 14^{108}$$

La **deuxième étape** consiste à construire la table des puissances qui décompose notre calcul. On commence avec le nombre de notre base : 14, puis on l'élève au carré  $14^2 = 196$  et ensuite on applique notre modulo  $196 \equiv 20 \pmod{22}$  et on répète l'opération en reprenant à chaque fois le résultat d'avant. On trouve cette table :

$$\begin{aligned}
14 &= 14 \\
14^2 &= 14^2 = 196 \Rightarrow 20 \\
14^4 &= 20^2 = 400 \Rightarrow 4 \\
14^8 &= 4^2 = 16 \Rightarrow 16 \\
14^{16} &= 16^2 = 256 \Rightarrow 14 \\
14^{32} &= 14^2 = 196 \Rightarrow 20 \\
14^{64} &= 20^2 = 400 \Rightarrow 4
\end{aligned}$$

La **troisième étape** consiste maintenant à évaluer le résultat de notre calcul du tout début.

$$14^{64} * 14^{32} * 14^8 * 14^4 = 14^{108}$$

$$14^{108} \equiv (4 * 20 * 16 * 4) \equiv 5120 \equiv 16 \pmod{22}$$

## Chiffrement/déchiffrement avec le RSA

La clé publique se compose de deux variables, les variables  $e$  et  $n$  qui sont une partie des données que nous avons interceptée avec le message chiffré. La clé privée se compose elle aussi de deux variables, la variable  $d$  (ce que nous cherchons à découvrir) et  $n$ . La variable  $n$  est le produit de deux nombres premiers  $p$  et  $q$ , c'est avec ces deux variables composant  $n$  ( $n$  est un nombre semi-premier) que nous pouvons calculer  $d$ .

$$n = pq$$

$$d = e^{-1} \pmod{(p-1)(q-1)} \text{ (il existe forcément un inverse modulaire car } e \text{ et } (p-1)(q-1) \text{ sont premiers entre eux)}$$

Pour chiffrer les données  $M$  avec RSA, il faut utiliser la formule suivante :  $M^e \pmod{n}$

Pour déchiffrer les données  $\mu$  avec RSA, il faut utiliser la formule suivante :  $\mu^d \pmod{n}$

## Méthode de résolution

Dans cette section, nous allons séparer notre raisonnement en 4 étapes. Dans la première étape, on cherche à trouver  $p$  et  $q$  en fonction de  $n$ , la deuxième étape consiste à calculer la clé privée (variable  $d$ ), la troisième à déchiffrer le message et finalement la dernière étape à reconstituer le message en décodant les données en UTF-8.

### Étape 1 : trouver les variables $p$ et $q$ en fonction de $n$

$n$  étant un nombre semi-premier, deux nombres premiers le composent, ces nombres sont  $p$  et  $q$ . Pour trouver  $p$  et  $q$ , il faut soit trouver  $p$  soit  $q$ , car si on trouve  $p$  on peut alors trouver  $q$  de la manière suivante :  $q = \frac{n}{p}$  et inversement.

Donc nous voulons trouver seulement  $p$ , pour ce faire nous essayons de diviser  $n$  par tous les nombres entre 2 et  $\sqrt{n}$ , on s'arrête dès que l'on trouve un nombre qui divise  $n$  sans reste. Nous nous permettons d'utiliser la force-brute, car on travaille sur un RSA-32 (32 bits),  $p$  et  $q$  font 16 bits chacun, la valeur maximale d'un nombre 16 bits est  $2^{16} - 1 = 65535$  donc si 65535 est un nombre premier on fait au maximum 65535 tours de boucle (et tests de division) sachant que 65535 n'est pas un nombre premier, notre programme fait de tout manière moins de 65535 itérations pour trouver  $p$ .

Dans notre cas, nous avons trouvé  $p = 38039$  et  $q = \frac{1653973759}{38039} = 43481$

## Étape 2 : calculer la clé privée (variable $d$ )

Une fois les variables  $p$  et  $q$  trouvées, on peut facilement calculer la variable  $d$  (clé privée) avec la formule suivante :  $d = e^{-1} \mod (p-1)(q-1)$

Dans notre cas, nous avons trouvé  $d = 679327809$

## Étape 3 : déchiffrer le message

Pour déchiffrer le message, on applique la formule de déchiffrement (qui pour rappel est :  $\mu^d \mod n$ ) où  $\mu$  sont les données chiffrées,  $d$  la clé privée et  $n$  le produit de  $p$  et  $q$  sur chacun des nombres que nous avons interceptés qui sont les suivants :

1511395078, 260436590, 1630654276, 1190458520, 790492067, 515550941, 297140366, 755589582, 647075331, 1191707844, 901889430, 660956124, 1500654109, 984322720, 1275630738, 1244853107, 1445928913, 1312523810, 265093060, 933013993, 1375592761, 195866064, 534502441, 928270408, 166404031, 621272622, 1304987439, 905393335, 55120151, 772595721, 506609577, 1172751778, 162439707, 233959833, 1468937795, 1358701120, 901889430, 495995733, 1524090698, 1043509086, 934992314, 1545639379, 1061595897, 1348452679, 1135067876, 905393335, 621272622, 55120151, 233959833, 1220119699, 708711266, 517797467, 195866064, 1579814353, 412378626, 498875436, 445485200, 7656659.

Par exemple pour déchiffrer le premier nombre 1511395078 des données chiffrées, on applique la formule de déchiffrement :

$$1511395078^{679327809} \mod 1653973759 = 2123076$$

Force est de constater que sans l'algorithme d'exponentiation rapide, il est impossible d'effectuer ce calcul rapidement même sur ordinateur moderne. On applique le déchiffrement sur toutes les données et on obtient une liste de nombres qu'il va falloir encore décoder.

## Étape 4 (étape final) : décoder les données déchiffrées

Voici les données déchiffrées : 2123076, 7696244, 544433524, 24934, 7317443, 539784046, 544433516, 11125618, 6909557, 544435823, 2123108, 1411408236, 7103073, 5382245, 6581871, 660807781, 544502629, 7693668, 6692984, 544434543, 544366960, 6909805, 1142959731, 744713839, 543781664, 2123116, 543384941, 2124905, 544500068, 7499873, 762554563, 1634559332, 2125417, 2138307, 7496048, 544369012, 2123108, 7233892, 6561907, 544765285, 7696234, 539784050, 6911347, 7233910, 661856372, 2124905, 2123116, 544500068, 2138307, 2122092, 544106854, 2127204, 6909805, 2108531, 543270851, 7366002, 7631471, 11877

Il faut donc maintenant décoder ces données en UTF-8 pour reconstituer le message textuel.

Par exemple, le nombre 2123076 correspond aux lettres "De", le nombre 7696244 correspond "tou", etc. Une fois qu'on concatène tous les bouts de chaîne de caractère, on obtient *le précieux message qu'on souhaite déchiffrer depuis le début.*

## Résultat

Dans cette section, nous allons aborder les résultat obtenus.

## Sortie

En appliquant notre méthode de résolution aux données interceptées, voici le message que nous avons trouvé :

***De toutes façons, les réunions de la Table Ronde c'est deux fois par mois. Donc, si le mec il dit après-demain à partir de dans deux jours, suivant s'il le dit à la fin du mois, ça reporte.***

## Performances

Étant donné que la clé a été générée sur une faible quantité de bits, on peut appliquer la méthode de force-brute pour la résolution de  $p$  et  $q$ .

## Explication

La raison pour laquelle on arrive à déchiffrer le message aussi rapidement est due au fait que  $n$  est codé sur une faible quantité de bits (32 pour être précis), ce qui nous permet de calculer  $p$  et  $q$  rapidement. Grâce à l'exponentiation rapide, on peut déchiffrer chaque partie du message rapidement du fait que l'on travaille avec de petits nombres.

## Conclusion

Le but principal de ce travail pratique était de déchiffrer un message chiffré avec RSA à l'aide des outils mathématiques que nous connaissons. Ces derniers sont :

- le théorème de Bachet-Bézout ;
- le théorème de Bézout ;
- l'inverse modulaire ;
- l'exponentiation modulaire ;
- RSA.

Ces outils utilisent l'arithmétique modulaire ce qui nous permet de travailler avec des nombres bien plus petits que ceux sortant des calculs bruts et d'éviter le problème de dépassement d'entier.

Nous avons trouvé plusieurs valeurs qui ont été essentielles pour le déchiffrement du message. La première fut  $p$  que l'on a trouvée en essayant de diviser  $n$  par tous les nombres entre 2 et  $\sqrt{n}$ , la valeur que nous avons trouvée pour  $p$  est 38039. Par conséquent, nous avons trouvé que  $q = \frac{1653973759}{38039} = 43481$

Ensuite, nous devons calculer la clé privée. Pour ce faire, nous l'avons calculée avec la formule suivante  $d = e^{-1} \bmod (p-1)(q-1)$  et avons trouvé que  $d$  vaut 679327809. Grâce à cette information cruciale, nous avons pu déchiffrer le message avec cette formule :  $\mu^d \bmod n$ . Nous l'avons appliquée sur chacune des données chiffrées que nous avons interceptées, ce qui nous a permis de déchiffrer le message.

Au niveau des améliorations possibles :

- il est clair que notre méthode de force-brute ne fonctionne que sur des RSA avec de petites clés (faibles en bits), nous pourrions appliquer d'autres méthodes pour casser le RSA qui serait bien plus efficace ;
- on pourrait prendre le projet et le réaliser dans le sens inverse étant donné que nous connaissons comment déchiffrer un message chiffré en RSA-32, nous savons donc aussi chiffrer un message.

Pour conclure, nous avons pu déchiffrer le message que nous avons intercepté en appliquant nos connaissances sur le fonctionnement du chiffrement RSA et des outils mathématiques qui l'entourent.