Mathématiques en technologies de l'information 1

Chapitre 2
Notions de Cryptographie

Quelques notions de théorie des nombres supplémentaires et utiles

L'utilisation de nombres et de calculs remonte aux origines de l'humanité.

Les premières traces de leur étude remontent à 1800 Av J.-C. (liste de triplets tels que $a^2 + b^2 = c^2$).

Il existe de nombreux problèmes dits «ouverts», facile à comprendre mais qui n'ont pas encore été prouvés.

… mais surtout, la théorie des nombres est une base indispensable à la cryptographie !!!

Quelques notions de théorie des nombres supplémentaires et utiles

Exemples :

- Existe-t-il une infinité de nombres *premiers jumeaux* ? (p premier et $p+2$ également) ?
- Conjecture de Goldbach : tout entier pair ≥ 4 peut s'écrire comme la somme de deux premiers.

Un exemple très célèbre

<u>Conjecture de Fermat (1601-1655):</u>

L'équation $x^n + y^n = z^n$ n'a pas de solution entière strictement positive pour $n > 2$.

Fermat dit : *« J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir. »*

La preuve officielle n'arrivera qu'en 1995 par Andrew Wiles, après 350 ans de tentatives infructueuses… Et ladite preuve s'étend sur plus de 1000 pages !

Quelques principes élémentaires

- Il existe une infinité de nombre premiers, mais…

- Existe-t-il un moyen de les générer ?
  Aucune formule n'existe pour TOUS les générer,
  Il est prouvé qu'il n'existe aucun polynôme non constant $P(n)$ tel que $P(n)$ soit premier pour tout n assez grand
  On ignore s'il existe un polynôme permettant de générer une infinité de nombres premiers !

- Crible d'Eratosthène
  Dans une tables de nombres de 1 à N, éliminer successivement tous les multiples des nombres premiers antérieurs

Exercice : appliquer le crible d'Eratosthène pour N = 100.

Quelques principes élémentaires

- Pour vérifier qu'un nombre n est premier, aucun nombre premier de 2 à $\sqrt{n}$ n'est diviseur de n.

- Quel est le plus grand nombre premier connu ?

On étudie les nombres de Mersenne $2^p - 1$ avec p premier
Projet GIMPS (Great Internet Mersenne Prime Search)
www.mersenne.org (oct. 2018)
(Mercenne est un mathématicien Français du XVII^{e} s.)

Today's Numbers	
Teams	1,253
Users	197,810
CPUs	1,761,953
TFLOP/s	331.917
GHz-Days	165,959

26 Déc. 2017 : $2^{77,232,917} - 1$ est premier !
C'est le 50^{e} nombre de Mersenne !
23.2 Mio de caractères !
Plus de 9000 pages !

Quelques principes élémentaires

Définition:

Deux nombres entiers a et b sont dits premiers entre eux si

$$PGCD(a, b) = 1$$

PGCD = Plus Grand Commun Diviseur

Le PGCD et les nombres premiers entre eux sont des fondamentaux pour la cryptographie (nous verrons certains exemples plus tard).

Méthode d'Euclide

<u>Calcul du PGCD selon la méthode d'Euclide</u>

Pour le calcul de $PGCD(a, b)$, nous supposerons (sans perte de généralité) que $a \geq b$

1. Calculer $r = a \; mod \; b$
2. Tant que $(r > 1)$ faire
   - Stocker $res \leftarrow r$
   - Redéfinir les variables $a \leftarrow b$, $b \leftarrow r$
   - $r = a \; mod \; b$
3. Si $r = 0$, alors $PGCD(a, b) = res$
   Si $r = 1$, alors $PGCD(a, b) = 1$ (a et b sont premiers entre eux)

Théorème Fondamental de l'arithmétique (Gauss, 1777-1855)

Tout nombre entier $\mathrm{n} \in \mathbb{N}, \mathrm{n} \geq 2$ peut être écrit comme un produit fini de nombres premiers.

(la preuve ne sera pas donnée dans ce cours !)

Celle-ci s'appelle la *décomposition en facteurs premiers* !

Factorisation en nombres premiers

La factorisation d'un nombre $a \in \mathbb{N}$ se base sur du «trial-and-error» en passant, itérativement, les diviseurs premiers…

- Tant que $a \; mod \; 2 = 0$, effectuer $a \leftarrow a/2$;
- Si $a \; mod \; 2 \neq 0$, alors passer au premier suivant (3) et tant que $a \; mod \; 3 = 0$, effectuer $a \leftarrow a/3$;
- Continuer jusqu'à ce que $a = 1$.

Cette approche est extrêmenet coûteuse !!!

Exemple

$$32 = 2 \times 2 \times 2 \times 2 \times 2 = 2^5$$

$$168 = 2 \times 2 \times 2 \times 3 \times 7 = 2^3 \times 3 \times 7$$

$$770 = 2 \times 5 \times 7 \times 11$$

Calcul du PPCM

$PPCM(a,b)$ (**P**lus **P**etit **C**ommun **M**ultiple) de deux nombres a et b est le plus petit entier naturel r tel que

a divise r ($r \; mod \; a = 0$) et
b divise r ($r \; mod \; b = 0$).

Comment calculer le PPCM ?

Méthode 1:
A l'aide de la décomposition en facteurs premiers de a et b :
$PPCM(a,b)$ est le produit de TOUS les facteurs COMMUNS

Calcul du PPCM

$PPCM(a, b)$ (<u>**P**</u>lus <u>**P**</u>etit <u>**C**</u>ommun <u>**M**</u>ultiple) de deux nombres a et b est le plus petit entier naturel r tel que

a divise r ($r \ mod \ a = 0$) et
b divise r ($r \ mod \ b = 0$).

Comment calculer le PPCM ?

<u>**Méthode 1:**</u>
A l'aide de la décomposition en facteurs premiers de a et b :
$PPCM(a, b)$ est le produit de TOUS les facteurs COMMUNS

Calcul du PPCM

$PPCM(a, b)$ (**<u>P</u>**lus **<u>P</u>**etit **<u>C</u>**ommun **<u>M</u>**ultiple) de deux nombres a et b est le plus petit entier naturel r tel que

a divise r ($r \; mod \; a = 0$) et
b divise r ($r \; mod \; b = 0$).

Comment calculer le PPCM ?

<u>Méthode 1:</u>
A l'aide de la décomposition en facteurs premiers de a et b :
$PPCM(a, b)$ est le produit du plus grand nombre de tous les facteurs présent dans les deux décompositions.

Exemple

$32 = 2 \times 2 \times 2 \times 2 \times 2 = 2^5$

$168 = 2 \times 2 \times 2 \times 3 \times 7 = 2^3 \times 3 \times 7$

$770 = 2 \times 5 \times 7 \times 11$

- $PPCM(32, 168) = 2^5 \times 3 \times 7 = 672$
- $PPCM(168, 770) = 2^3 \times 3 \times 5 \times 7 \times 11 = 9240$

Propriété intéressante

Pour toute paire de nombres $a, b \in \mathbb{N}$, on a que

$$a \times b = PGCD(a, b) \times PPCM(a, b)$$

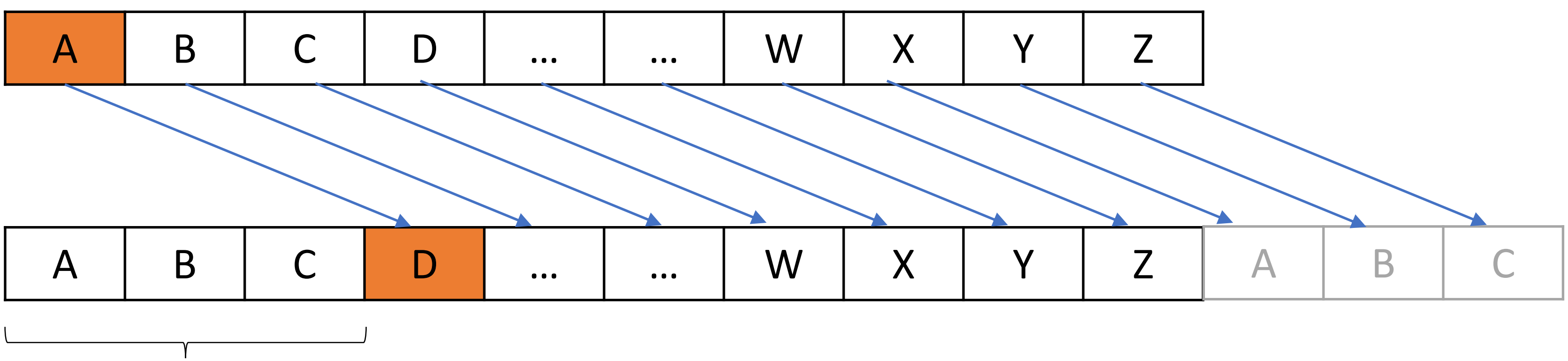
Autrement dit : si on connait $a \times b$ et $PGCD(a, b)$, alors

$$PPCM(a, b) = \frac{a \times b}{PGCD(a, b)}.$$

Quel est l’intérêt des nombres premiers ?

Il sont à l’origine des méthodes de cryptographie modernes !

La première méthode de cryptage communément admise est le Chiffre de César (chiffrement par décalage)



Le chiffre de César est ici de 3.

Exemple

Cryptage de «HEPIA» avec le Chiffre de César = 11
Astuce : passage par les nombres avec a = 1, b=2, …

H	E	P	I	A
8	5	16	9	1

19	16	1	20	11
S	P	A	T	K

Exemple

Quelle est la formule pour cette transformation ?

x_1	x_2	x_3	…	x_N

$$y_i = 1 + (x_i + N_{César}) mod\ 26$$

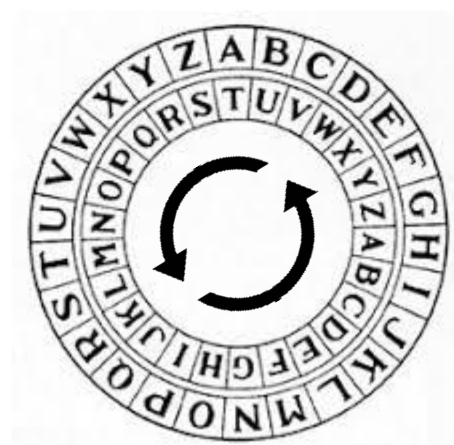
y_1	y_2	y_3	…	y_N

Cela vous semble-t-il connu ?

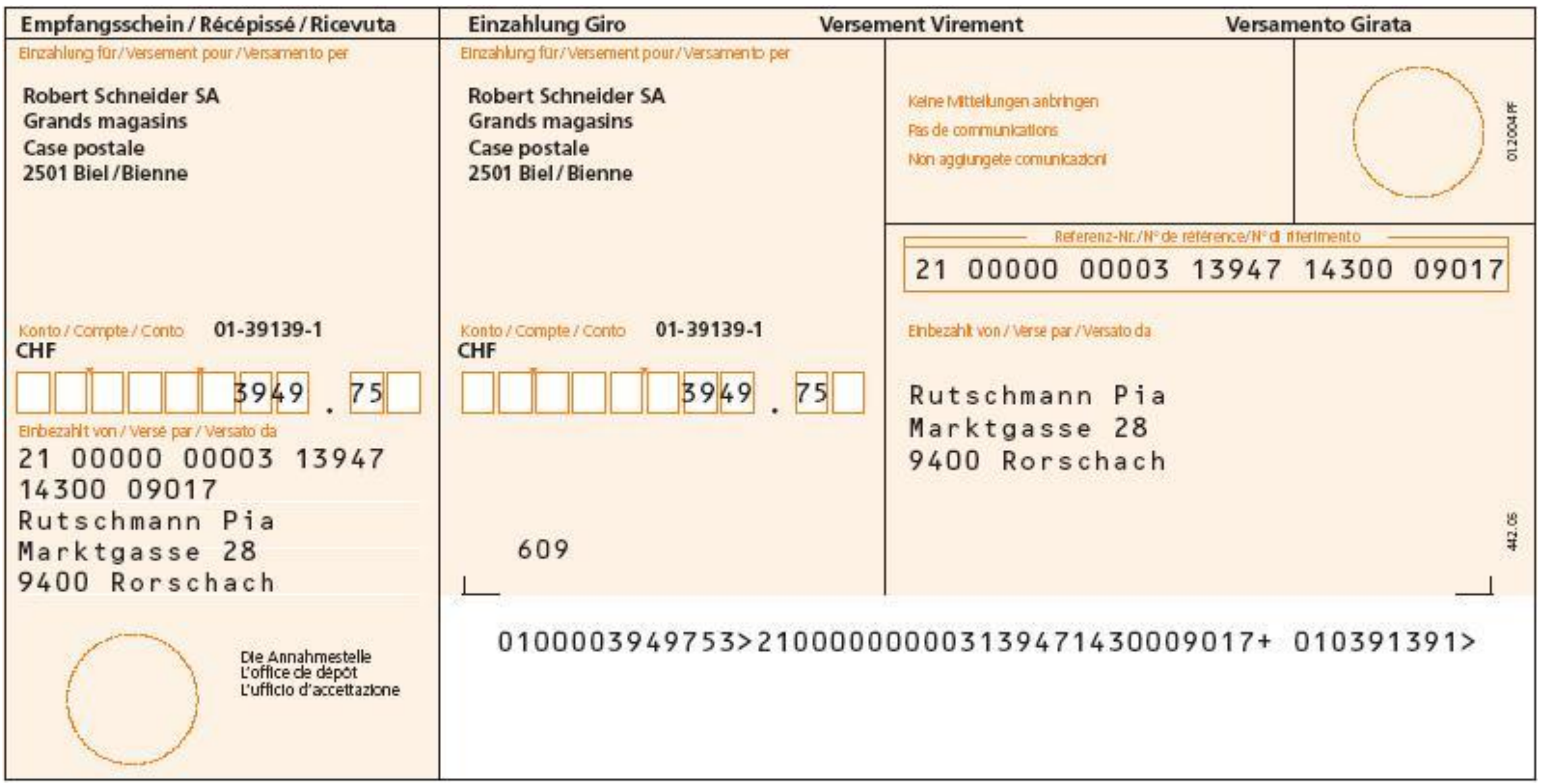
Cela ressemble fortement à la somme sur un nombre de bits finis (avec overflow) !!!

Exercice :

Prouver que tout nombre de César est équivalent à un nombre entre 0 et 26.



Un exemple peu connu mais très utilisé en Suisse…



Empfangsschein / Récépissé / Ricevuta

Einzahlung für / Versement pour / Versamento per

Robert Schneider SA
Grands magasins
Case postale
2501 Biel / Bienne

Konto / Compte / Conto 01-39139-1

CHF 3949 . 75

Einbezahlt von / Versé par / Versato da

21 00000 00003 13947
14300 09017
Rutschmann Pia
Marktgasse 28
9400 Rorschach

Die Annahmestelle
L'office de dépôt
L'ufficio d'accettazione

Einzahlung Giro — Versement Virement — Versamento Girata

Einzahlung für / Versement pour / Versamento per

Robert Schneider SA
Grands magasins
Case postale
2501 Biel / Bienne

Konto / Compte / Conto 01-39139-1

CHF 3949 . 75

609

Keine Mitteilungen anbringen
Pas de communications
Non aggiungete comunicazioni

012004 PF

Referenz-Nr. / N° de référence / N° di riferimento

21 00000 00003 13947 14300 09017

Einbezahlt von / Versé par / Versato da

Rutschmann Pia
Marktgasse 28
9400 Rorschach

442.06

0100003949753>210000000003139471430009017+ 010391391>

Algorithme Modulo 10 récursif

Il permet de vérifier si une séquence de chiffres contient une erreur.

- Soit la table de reports définie comme suit :

$Table =$

0	9	4	6	8	2	7	1	3	5

- Initialiser $r = 0, i = 0$

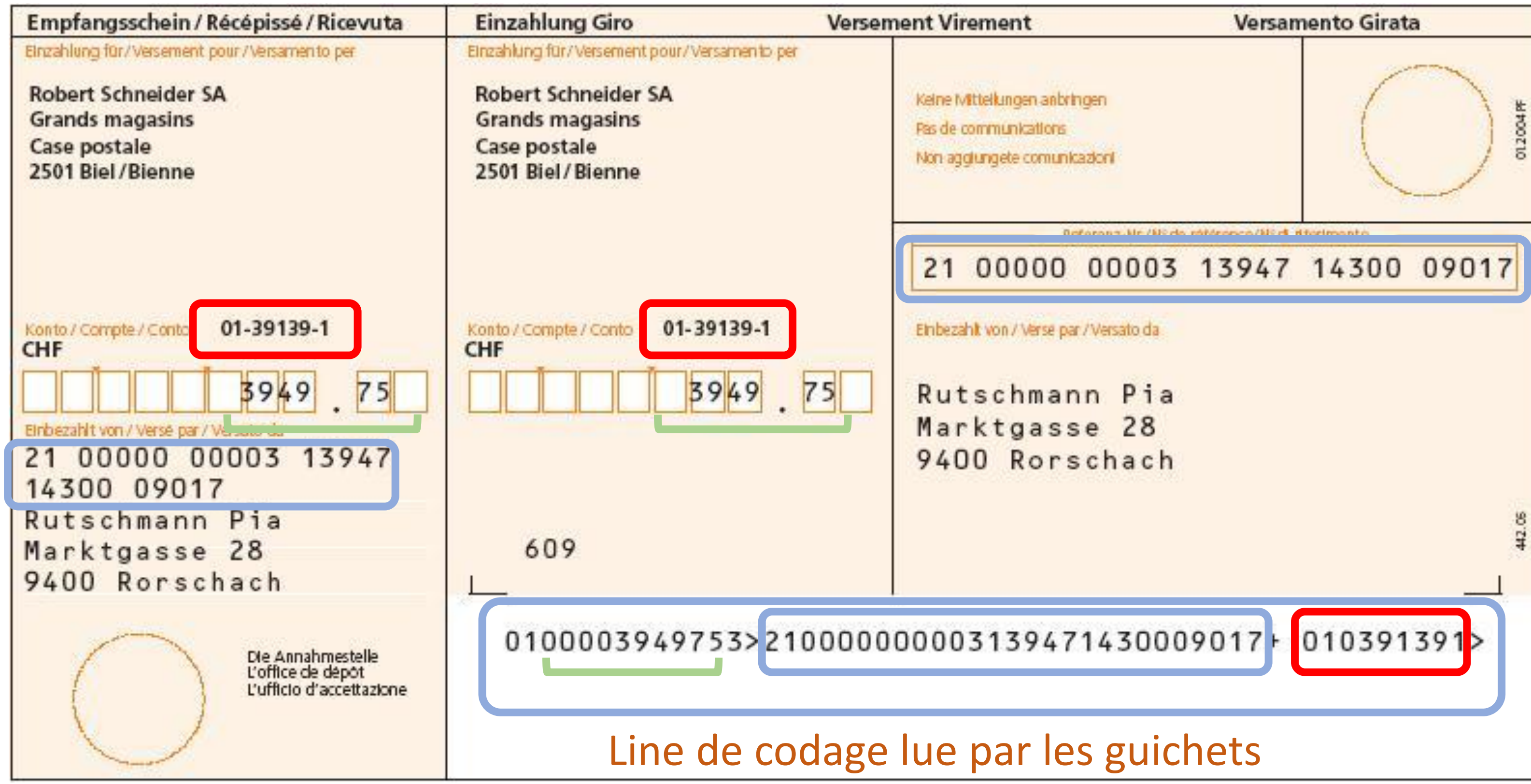
- Pour chaque chiffre x_i dans la séquence

  $r = Table[(x_i + r) \bmod 10]$

  $i = i + 1$

  Si $i > \#chiffres$: STOP : retourner $10 - r\ mod\ 10$.

Ce qu'on voit sur les BVR



Décomposition de la ligne de codage BVR

0100003949753>210000000003139471430009017+ 010391391>

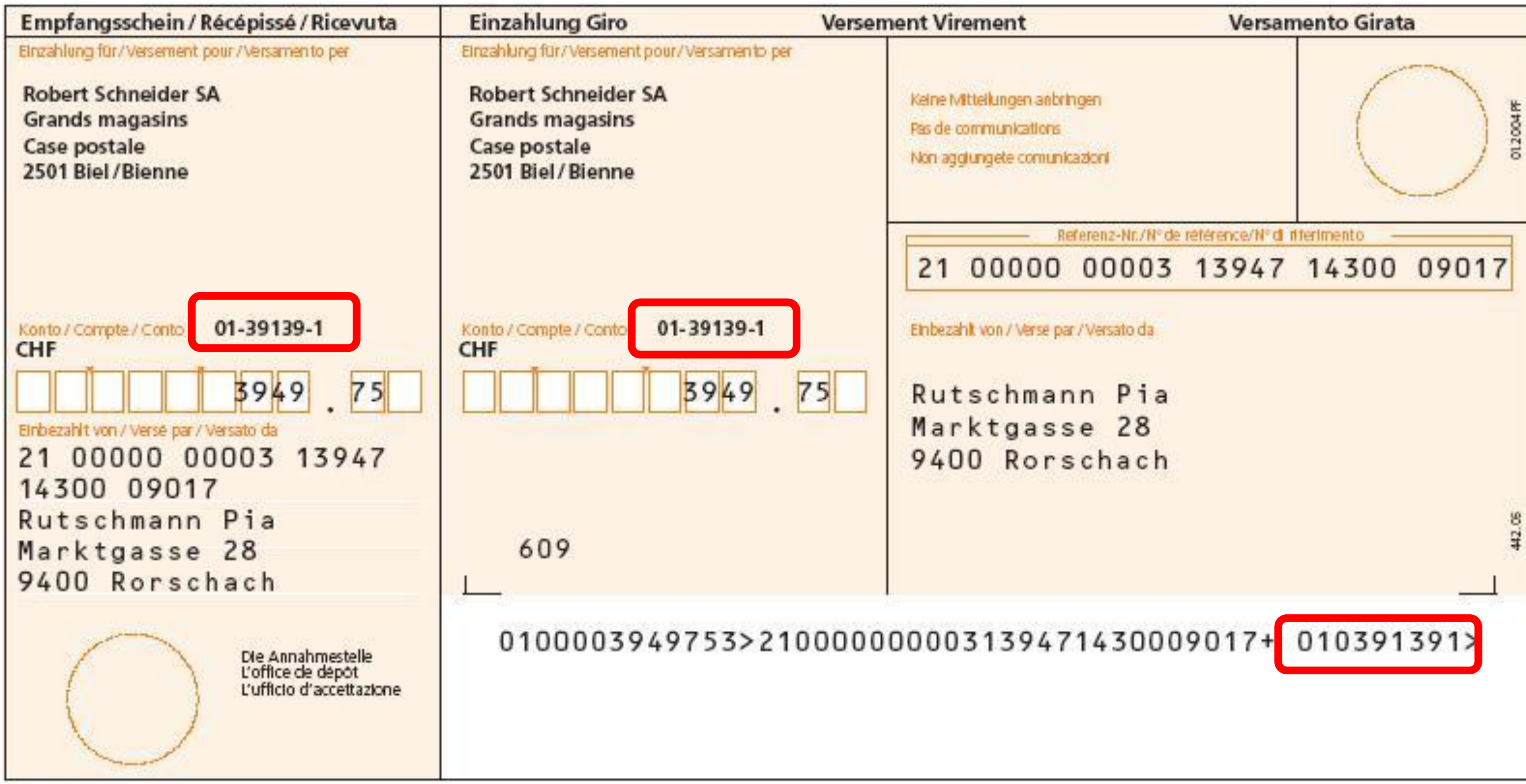
01	**000394975**	**3**	**>**	**21000000000313947143000901**	**7**	**+**	**01039139**	**1**	**>**
Code	Montant * 10 sur 9 chiffres (0 à gauche)	CLE		Code contenant des données internes (p.ex. référence du compte, numéro client, numéro de facture, date, …) Il existe des variantes avec 26 ou 15 positions !	CLE		Numéro de compte sur 2 + 7 chiffres (0 à gauches)	CLE	

Il y a trois clés, toutes calculés avec l'algorithme modulo 10 récursif :

- La clé du montant (**3** – clé obtenue avec les 11 chiffres précédents),
- Clé du numéro de réf. (**7** – clé obtenue avec les 26 chiffres précédents),
- Clé du numéro de CCP (**1** – clé obtenue avec les 9 chiffres précédents).

Exemple : codage du CCP

Appliquons l'algorithme Modulo 10 récursif pour vérifier le numéro de compte 01–39139–1


Empfangsschein / Récépissé / Ricevuta
Einzahlung für / Versement pour / Versamento per
Robert Schneider SA
Grands magasins
Case postale
2501 Biel / Bienne
Konto / Compte / Conto 01-39139-1
CHF
3949 . 75
Einbezahlt von / Versé par / Versato da
21 00000 00003 13947
14300 09017
Rutschmann Pia
Marktgasse 28
9400 Rorschach
Die Annahmestelle
L'office de dépôt
L'ufficio d'accettazione

Einzahlung Giro Versement Virement Versamento Girata
Einzahlung für / Versement pour / Versamento per
Robert Schneider SA
Grands magasins
Case postale
2501 Biel / Bienne
Konto / Compte / Conto 01-39139-1
CHF
3949 . 75
Keine Mitteilungen anbringen
Pas de communications
Non aggiungete comunicazioni
Referenz-Nr./N° de référence/N° di riferimento
21 00000 00003 13947 14300 09017
Einbezahlt von / Versé par / Versato da
Rutschmann Pia
Marktgasse 28
9400 Rorschach
609
0100003949753>210000000003139471430009017+ 010391391>

Exemple : codage du CCP

- D'abord, notons que le CCP est codé sur 2 + 7 chiffres + le chiffre clé, or 01-39139-**1** est composé de 2 + 6 chiffres,

- Il manque un 0 : 01-039139-**1**,

- Il faut donc vérifier si la séquence 01039139 retourne bien **1** comme clé de chiffrement !

Clé du CCP 01-(0)39139-?

$T =$

0	9	4	6	8	2	7	1	3	5

i	r	x_i	$v = (x_i + r) \bmod 10$	$r = T[v]$	**Clé** $10 - r \; mod \; 10$
0	0	0	$(0 + 0) \bmod 10 = 0$	0	0
1	0	1	$(1 + 0) \bmod 10 = 1$	9	1
2	9	0	$(0 + 9) \bmod 10 = 1$	5	5
3	5	3	$(3 + 5) \bmod 10 = 8$	3	7
4	3	9	$(9 + 3) \bmod 10 = 2$	4	6
5	4	1	$(1 + 4) \bmod 10 = 5$	2	8
6	2	3	$(3 + 2) \bmod 10 = 5$	2	8
7	2	9	$(9 + 2) \bmod 10 = 1$	9	**1**

STOP : retourner **1**

Petit Théorème de Fermat

Soit p un nombre premier, alors et tout $a \in \mathbb{Z}$ non-divisible par p, on a

1. $(a^p)\ mod\ p\ \ = (a)\ mod\ p,$

2. $(a^{p-1})\ mod\ p\ = 1,$

3. pour tout $a \in \mathbb{Z}$ qui n'est pas multiple de p,
   $(a^{p-1})\ mod\ p = (a\ )\ mod\ p\ ,$

4. pour tout $a \in \mathbb{Z}$ qui n'est pas multiple de p, il existe un entier $k \in \mathbb{N}^*$ tel que $(a^k)\ mod\ p = 1$. De plus, le plus petit $k > 0$ vérifiant cette égalité divise $p - 1$.

Exercice

Vérifiez les propriétés avec les paires suivantes :

1. $a = 7, p = 5,$

2. $a = 10, p = 3.$

Méthode d'Euclide étendue

Soient $a, b \in \mathbb{N}^*$ avec $a, > b$ (sans perte de généralité), trouvons les coefficients de Bézout $x, y \in \mathbb{Z}^*$ tels que

$$PGCD(a, b) = x \times a + y \times b$$

<u>Algorithme:</u>

0) $r_0 = a = x_0 \times a + y_0 \times b$ $\quad$ $r_0 = a, x_0 = 1, y_0 = 0$

1) $r_1 = b = x_1 \times a + y_1 \times b$ $\quad$ $r_1 = b, x_1 = 0, y_1 = 1$

Tant que $r_i \neq 0$ faire

i) Résoudre $r_i = r_{i-2} - q_i \times r_{i-1}$ (par la division euclidienne)

Poser $x_i = x_{i-2} - q_i \times x_{i-1}$

Quand $r_i = 0$, alors $r_{i-1} = PGCD(a, b)$, $x = x_{i-1}$ et $y = y_{i-1}$

Exemple

Calculer $PGCD(168,\ 68) = x \times a + y \times b$

<u>Algorithme:</u>

0) $r_0 = 168, x_0 = 1, y_0 = 0$
1) $r_1 = 68,\ \ x_1 = 0, y_1 = 1$

2) $\mathrm{r}_2 = 32 = 168 - 2 \times 68$ ($q_2 = 2$)
Poser $x_2 = x_0 - 2 \times x_1 = 1 - 2 \times 0 = 1$
et $y_2 = y_0 - 2 \times y_1 = 0 - 2 \times 1 = -2$

Exemple $PGCD(186,\ 68) = x \times a + y \times b$

3) $\mathrm{r}_3 = 4 = 68 - 2 \times 32$ ($q_3 = 2$)
Poser $x_3 = x_1 - 2 \times x_2 = 0 - 2 \times 1 = -2$
et $y_3 = y_1 - 2 \times y_2 = 1 - 2 \times (-2) = 5$

4) $\mathrm{r}_4 = 0 = 32 - 8 \times 4$

Réponse : $PGCD(186, 68) = 4 = -2 \times 168 + 5 \times 68$,
Les coefficients de Bézout sont $[-2; 5]$.

Algorithme de chiffrement RSA

Par Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman (1977).

C'est une méthode de cryptage *ASYMÉTRIQUE*, contrairement au Nombre de César qui lui, est symétrique…

Quelle différence ?

Le nombre de César est basé sur une seule clé secrète (le nombre lui-même) qui, s'il est connu, permet de déchiffrer le message.

En tant que méthode asymétrique, RSA possède une clé privée ET une clé publique !

Principe asymétrique

1) Julie génère une clé publique $[n, e]$ et une clé privée $[d]$.

2) Paul écrit un message en clair (non-crypté) à Julie,

3) Le texte est converti en un nombre M (chaque caractère est remplacé par le code ASCII, Unicode, ….)
NOTE: il faut que $0 \leq M < n$, donc si $M \geq n$, on décomposera M en plusieurs nombres $M_i \in [0, n[$.

4) Paul récupère la clé publique de Julie, composée d'une paire et calcule $\mu = M^e mod\ n$,

5) Julie reçoit $\mu = M^e mod\ n$ et calcule $\mu^d = M^{e \times d} = M\ mod\ n$ pour déchiffrer les messages.

Génération des clés

Julie génère une clé publique $[n, e]$ et une clé privée $[d]$.

- Choix de deux nombres premiers p et q (très grands!),

- Calcul de $n = p \times q$: n est publique,

Ex: $p = 5$ et $q = 11$, alors $n = 55$

- Calcul de $\varphi(n) = (p-1) \times (q-1)$: $\varphi(n)$est privé

Ex: $p = 5$ et $q = 11$, alors $\varphi(n) = 40$

- Choix d'un exposant e tel que $\mathrm{pgcd}\big(e, \varphi(n)\big) = 1$,

Ex: $e = 7$ (qui est premier avec $\varphi(n) = 40$).

Génération des clés [suite]

- Comme $\mathrm{pgcd}\big(e, \varphi(n)\big) = 1$, par l'algorithme d'Euclide étendu on obtient les coefficients de Bézout pour
$$d \times e + b \times \varphi(n) = 1$$

Ou autrement dit $d \times e = 1 \; mod \; \varphi(n)$!

Ex: $\varphi(n) = 40$ et $\mathrm{e} = 7$ => $3 \times 40 - 17 \times 7 = 1$
Donc $\mathrm{d} = -17 \; mod \; 40 = 23$.

NOTE: si $\mathrm{d} < 0$, on prend $\mathrm{d} = \mathrm{d} \bmod \varphi(n)$.

Dans ce cas, la clé publique est $[n, e] = [55, 7]$ et la clé privée est $d = 23$.

Chiffrement du message

Paul écrit un message qu'il convertit en nombre $M = 13$ puis applique la clé publique de Julie $[n, e] = [55, 7]$

Paul calcule alors $\mu = m^e \; mod \; n = 13^7 \; mod \; 55 = 7$ via ***l'algorithme d'exponentiation rapide*** :

$$13^1 \; mod \; 55 = 13^1 \; mod \; 55 = 13$$
$$13^2 \; mod \; 55 = (13^1 \; mod \; 55) \times (13^1 \; mod \; 55) = 169 \; mod \; 55 = 4$$
$$13^4 \; mod \; 55 = 4 \times 4 \; mod \; 16 \; mod \; 55 = 16$$
$$\begin{aligned} 13^7 \; mod \; 55 &= (13^4 \times 13^2 \times 13^1) \; mod \; 55 = (16 \times 4 \times 13) \; mod \; 55 \\ &= 832 \; mod \; 55 = 7. \end{aligned}$$

Le message envoyé à Julie est donc $\mu = 7$.

Déchiffrement du message

Julie reçoit le message $\mu = 7$. Elle va alors calculer (via l'algorithme d'exponentiation rapide)

$$M = \mu^d \; mod \; n$$

$7^1 \; mod \; 55 = 7$
$7^2 \; mod \; 55 = (49 \; mod \; 55) = 49$
$7^4 \; mod \; 55 = 49 \times 49 \; mod \; 55 = 2401 \; mod \; 55 = 36$
$7^8 \; mod \; 55 = 36 \times 36 \; mod \; 55 = 1296 \; mod \; 55 = 31$
$7^{16} \; mod \; 55 = 31 \times 31 \; mod \; 55 = 961 \; mod \; 55 = 26$
$7^{23} \; mod \; 55 = (7^{16} \times 7^4 \times 7^2 \times 7^1) mod \; (26 \times 36 \times 49 \times 7) \; mod \; 55$
$= (936 \; mod \; 55) \times (343 \; mod \; 55) = (1 \times 13) \; mod \; 55$
$= 13.$

RSA – vue d'ensemble

Public $[n; e]$

M → Paul → $\mu = M^e \bmod n$ → Julie → $M = \mu^d \bmod n$

<u>Initialisation (privée) :</u>

$n = p \times q$ et

$PDGC(\varphi(n), e) = 1$

Avec $\varphi(n) = (p-1) \times (q-1)$

d coefficient de Bézout tel que

$$d \times e + c \times \varphi(n) = 1$$

Si $d < 0$, prendre $d = d \bmod \varphi(n)$

RSA - formalisation

Soit p, q deux premiers avec $p \neq q$ et

- $n = p \times q$,
- $\varphi(n) = (p-1) \times (q-1)$,
- e tel que $PGCD\big(e, \varphi(n)\big) = 1$,
- d tel que $d \times e = 1 \; mod \; \varphi(n)$

Alors pour tout $0 \leq M < n$ on a

Si $\boldsymbol{\mu = M^e \; mod \; n}$ alors $\boldsymbol{M = \mu^d \; mod \; n}$.

RSA – Complexité de décodage

En 1999, des chercheurs on décodé le RSA-155 (RSA avec nombre codé sur 155 chiffres décimaux, soit 512 bits).

Total : 8'000 ans de calculs à 1 Megaflops (1 millio d'opérations par secondes).

Résolu en 3 mois de calcul avec 300 ordinateurs PC dédiés.

Aujourd'hui, les RSA-1024 et 2048 sont souvent utilisés. Les techniques brutes sont inefficaces, mais il est possible de cracker la clé grâce à des mesures de variations électriques sur un PC (nécessite un accès physique) !

RSA – Complexité de décodage

Supposons que p et q soient de l'ordre de 10^{100} (ce qui es le cas pour le RSA-1024).

Alors pour effectuer la décomposition en nombres premiers de $p \times q$ (d'ordre 10^{200}) il faut au pire des cas $\sqrt{p \times q} = \sqrt{10^{200}} = 10^{100}$ calculs.

Imaginons que nous disposons d'une puissance totale de 10^{30} flops (c'est une estimation grossière de la capacité de calcul totale de TOUS les ordinateurs sur terre combinés).

Il faudrait alors 10^{70} secondes pour résoudre la décomposition, soit plus de 10^{63} années de calcul !!!

Comment générer p et q ?

La génération est basé sur une approche probabiliste (donc les deux nombres premiers sont «probablement» premiers)

1. Générer un nombre aléatoire de la longueur désirée, disons a
2. Appliquer le Test de Miller-Rabin pour vérifier si a est premier,
   OUI => choisir a comme premier
   NON => prendre $a = a + 1$ et recommencer 2.

Test de Miller-Rabin

ATTENTION: il ne s'agit pas d'un test EXHAUSTIF, mais PROBABILISTE

Si le test échoue, on sait que le nombre a n'est PAS premier.
S'il réussit, on dira que a est «probablement» premier.

Test de Miller-Rabin

Entrées:

- a un entier impair > 3 (le nombre à tester)
- k un paramètre déterminant la précision du test (nombre de fois)

Sortie:

Faux si a est factorisable, Vrai si a est probablement premier

Test de Miller-Rabin

Décomposer $a-1=2^s \times d$ (a étant impair, $a-1$ est un multiple de 2)

Pour $k=1,\ldots,n$ faire

    choisir aléatoirement $x \in [2, a-2]$ et $y = x^d \: mod \: a$

    Si $y \neq 1$ et $y \neq a-1$

        pour $r = 1, \ldots s-1$ faire

            $y = y^2 \: mod \: a$

            SI $y = n-1$ => passer à $k+1$

        fin

        SI $r = s$ et $y \neq 1$ => STOP, a n'est pas premier

        SINON passer à $k+1$

    fin

Fin => a est probablement premier

Test de Miller-Rabin - Exemple

Question: $a = 221$ est-il un nombre premier ?

- $a - 1 = 220 = 2 \times 110 = 2^2 \times 55$ ($s = 2$, $d = 55$)
- $x = 174 \in [2, 220]$ (pris aléatoirement) [Test $k = 1$]
  - $r = 1$:

    $y = x^d \, mod \, a = 174^{55} \, mod \, 221 = 47 \notin \{1,220\}$

  STOP: a n'est PAS premier

Exercice RSA

Appliquez le chiffrement et déchiffrement du RSA avec

- $p = 5$ et $q = 7$
- choisissez $e = 5$ (vérifiez que c'est un choix valide)
- (d = 5)
- Envoyez le message $M = 10$ (donc $10^5 \, mod \, 35 = 5$)