APRES-MIDI Cours du 07.12.2020

lundi, 7 décembre 2020 12:59

Application des mathématiques à la cryptographie

Chiffrer / Encoder vs Déchiffrer / décoder

Qui est considéré comme le père de la cryptographie ???

Le nombre de César : correspond à un décalage FIXE dans l'alphabet

0	1	2					25
A	B	C	...	...	W	X	Y	Z
D	E	F	...	...	Z	A	B	C

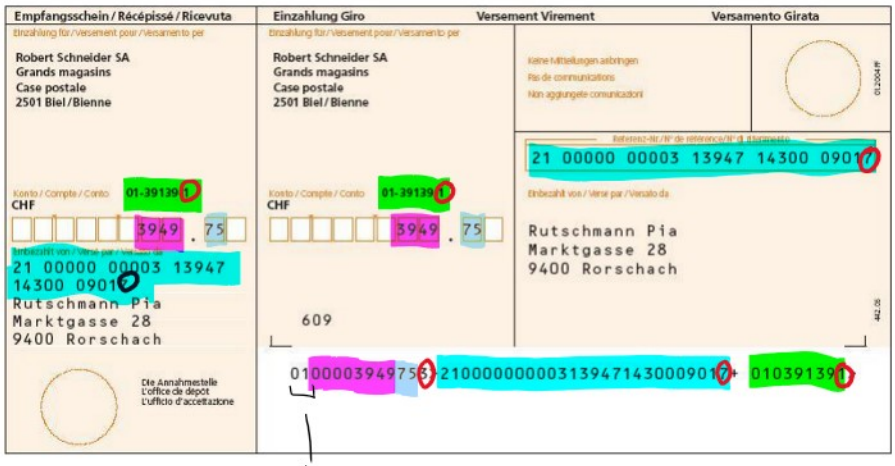
$N \equiv_{26} 3 \equiv_{26} 3+26 \equiv_{26} 29 \equiv_{26} 55$

$\equiv_{26} -23 \equiv_{26} -49$

Si je veux écrire la i^e lettre, elle est remplacée par

$i + N \mod 26$

2e Exemple : les BVR



Récépicé

Code transaction

CCP (N° compte)

Informations définies par le créancier

Montant

0 clés de "vérification" (Checksum)

Algo. Mod 10 Récursif.

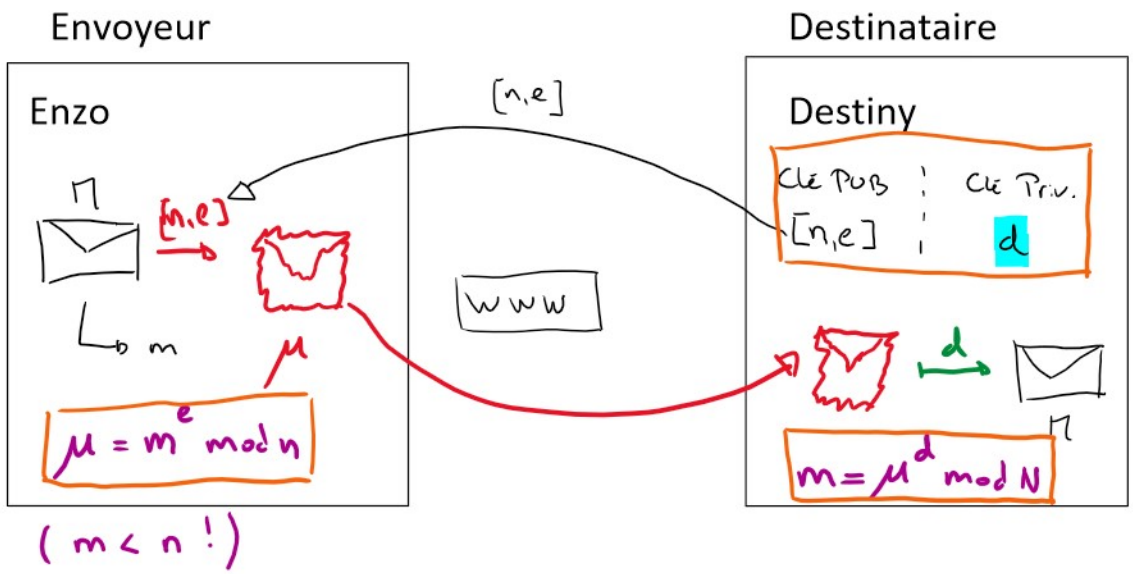
Police OCR-B 10

Une des premières applications de l'OCR (reconnaissance de charactères optique).

RSA :
Rivest, **S**hamir et **A**dleman (1977 MIT)

RSA est une méthode ASYMÉTRIQUE - il y a une clé PUBLIQUE ET une clé PRIVÉE.
A contrario, on dit le nombre de César est une méthode SYMÉTRIQUE, car la clé pour chiffrer est la même que celle pour déchiffrer les message !

Clé privée => décoder le message chiffré
Clé publique => encode le message "en clair"



$n, e, d, m, \mu \in \mathbb{N}$

M texte (m = "Bonjour")
↓ encodage ASCII UTF-8
$m \in \mathbb{N}$

Création des clés privées et publiques (par Destiny !)

1. Générer aléatoirement deux ***nombres premiers*** p et q qui sont différents ($p \neq q$)

2. $n = p \times q$

3. Calcule $\varphi(n) = \varphi(p \cdot q) \overset{\text{s.10}}{=} (p-1)(q-1)$

4. Choisit un e qui premier avec $\varphi(n)$

} clé publique !

5. Par Euclide étendu, on calcule les coefficients de Bézout

$$PGCD(e, \varphi(n)) = 1 = e \cdot x + \varphi(n) \cdot y$$

e : choisi premier avec $\varphi(n)$

Pose clé privée : $d = y \bmod \varphi(n)$

Eléments non déterministes (aléatoires) du processus de génération des clés sont : *p, q, e* suffisent pour retrouver les clés privées et publiques !!!!
On peut récupérer n et e, et n = p×q !!!

Toute la force du RSA réside dans la complexité de retrouver p et q sachant n !!

Craquer le RSA revient à factoriser n !!!!!!

Exemple : Enzo veut envoyer "Bonjour" à Destiny.

Destiny va générer sa paire de clés priv/pub

1. $p = 5$, $q = 11$

2. $n = p \cdot q = 5 \cdot 11 = 55$

3. $\varphi(n) = (p-1)(q-1) = \dots$

3. $\varphi(n) = (p-1)\cdot(q-1) = 4 \cdot 10 = 40$

4. Choisi $e = 7$ $(\text{PGCD}(7,40) = 1)$

5. Euclide étendu donne :

$\text{PGCD}(40,7) = 1 = 40 \cdot 3 + 7 \cdot (-17)$ (e = 7, y = (-17))

$d = (-17) \bmod 40 = 23 = d$

$[n, e] = [55, 7]$; $d = 23$

$\mu = m^e \bmod n$; $m = \mu^d \bmod n$

Enzo: reçoit [55,7] de Destiny, et il va encoder son message

"Bonjour" $\xrightarrow{\text{"Ascii"}}$ $m = 13$

$\mu = 13^7 \bmod 55 = 7$ (exp. rap.)

Destiny reçoit "7" et va le déchiffrer avec d=23

$m = 7^{23} \bmod 55 = 13 \xrightarrow{\text{"Ascii"}}$ "Bonjour" !