

Chiffrement : Le nombre de César

Considéré comme le premier algorithme de chiffrement

Définit un "nombre" N de 1 à 25 et on "encode" un message via un décalage de " N " lettres dans l'alphabet.

A	B	C	D	X	Y	Z
C	D	E	Z	A	B

$$N=2$$

Mathématiquement, qu'est-ce que cela nous donne ?

$$\text{Si on a une lettre } i, \text{ elle par } j = i + N \pmod{26} \quad (N=2)$$

Et pour le déchiffrer :

$$i = j - N \pmod{26} = (j + 26 - N) \pmod{26} \quad \begin{pmatrix} -2 \\ +24 \end{pmatrix}$$

Bulletin de versement

Empfangsschein / Récépissé / Ricevuta	Einzahlung Giro	Versement Virement	Versamento Girata
Bestellung für / Versement pour / Versamento per Robert Schneider SA Grands magasins Case postale 2501 Biel/Bienne	Bestellung für / Versement pour / Versamento per Robert Schneider SA Grands magasins Case postale 2501 Biel/Bienne	Keine Mitteilungen anbringen Pas de communications Non aggiungere comunicazioni	<input type="radio"/> 0120000F
Konto / Compte / Conto: CHF 01-39139-0 3949 . 75 Bestellung für / Versement pour / Versamento per 21 00000 00003 13947 14300 09017 Rutschmann Pia Marktgasse 28 9400 Rorschach	Konto / Compte / Conto: CHF 01-39139-0 3949 . 75 Bestellung für / Versement pour / Versamento per 609 01000039497-5 210000000003139471430009017 010391391	Bestellung für / Versement pour / Versamento per Rutschmann Pia Marktgasse 28 9400 Rorschach	<input type="radio"/> 0120000F
<p>Données remplies par l'émetteur du BVR</p> <p>Compte destinataire</p> <p>Ligne de codage OCR-B10</p> <p>Code de transaction</p> <p>Récipti</p>			

A B et C sont des "check sum"

A,B et C permettent de vérifier que les informations soient cohérentes !

Ils sont calculés avec l'algorithme mod 10 récursif (c.f. polycop).

LE RSA

Rivest, Shamir et Adleman (breveté en 1977 au MIT).

C'est un chiffrement ASYMÉTRIQUE, contrairement au Nombre de César qui est SYMÉTRIQUE.

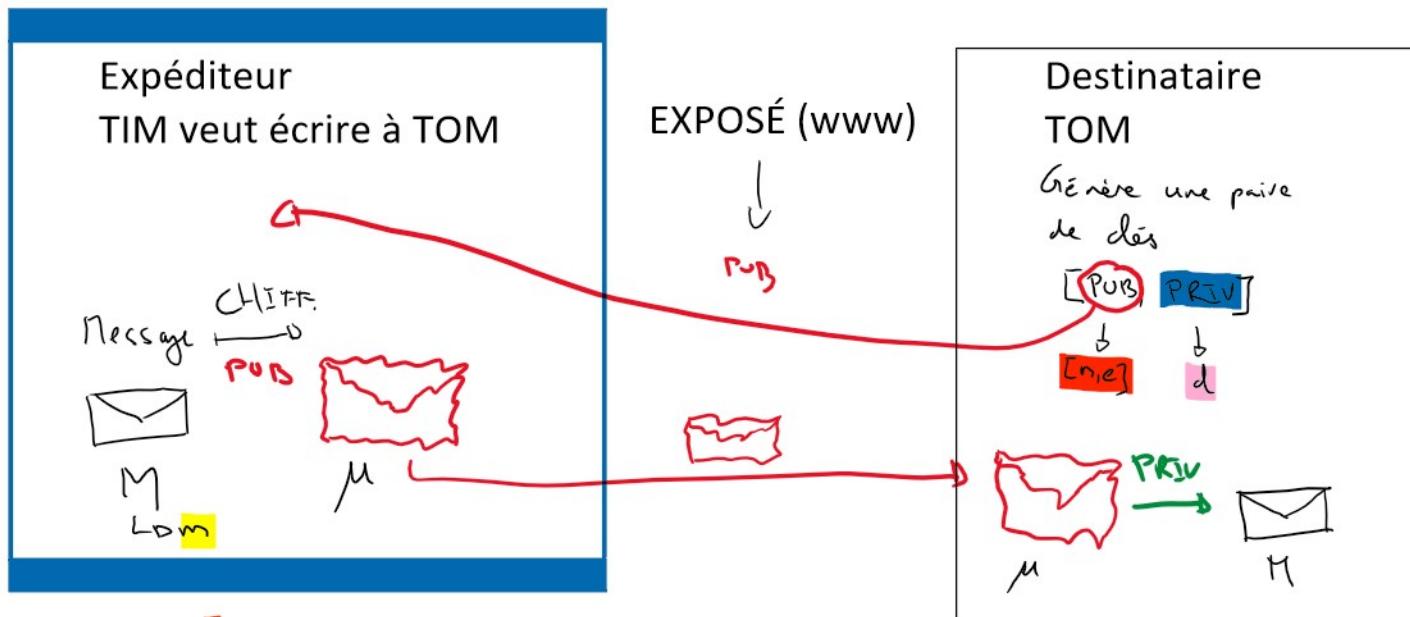
Car il y a une notion de "paires de clés", une clé PUBLIQUE, et une clé PRIVÉE.

Symétrique : la clé de chiffrement ET de déchiffrement est la même !!!

Risque => si on connaît la clé, le message est compromis !

Asymétrique : la clé publique est utilisée pour ENCODER (chiffrer) le message, alors que la clé privée est utilisée pour le DÉCODER (déchiffrer). Seule la clé publique est transmise, mais le message n'est PAS compris car seule la clé PRIVÉE permet de déchiffrer le message !!!!

Principe du RSA



$$M = m^e \pmod{n}$$

où $[n, e]$ clé publique

$$M \mapsto m = M^d \pmod{n}$$

M message d'origine (texte) => on le convertit en "nombre" m
(p.ex. représentation ASCII sur 16 bits)

⚠ m, n, e, M et $d \in \mathbb{N}$.
 $m < n$

Question : comment Tom (destinataire) doit-il choisir n, e et d ???

Tout repose sur 2 nombres premiers p et q !

Que fait Tom (destinataire)

1. Génère aléatoirement 2 nombres premiers p et q (premiers entre eux, $p \neq q$)
2. $n = p \times q$
3. Calcule $\varphi(n) = \varphi(p \cdot q) = (p-1) \cdot (q-1)$
4. Choisit e tel que $\text{PGCD}(e, \varphi(n)) = \text{PGCD}(e, (p-1) \cdot (q-1)) = 1$
5. On utilise Euclide étendu pour calculer les coeff. De Bézout

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

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

$$d = x \bmod \varphi(n)$$

Exemple :

Choisissons p et q $p = 5$, $q = 11$

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

$$2. \quad n = 5 \cdot 11 = 55$$

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

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

$$5. \quad 1 = 7 \times (-17) + 40 \times 3$$

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

Que fait Tim (expéditeur)

"Bonjour" $\xrightarrow{\text{"ASCII"}}$ 13

$M \Rightarrow (\text{ascii}) \dots m = 13$

$$\mu = m^e \bmod n = 13^7 \bmod 55 = 7$$

Du côté de TOM :

$$\mu \mapsto m = \mu^d \bmod n = 7^{23} \bmod 55 = 13 \xrightarrow{\text{"ASCII"}} \text{"Bonjour"!}$$