Le numéro INSEE d'une personne est composé de 15 chiffres : les 13 premiers forment un nombre N qui identifie la personne et les deux derniers forment une clé C calculée ainsi : C = 97 – *r* où *r* est le reste de N dans la division par 97.
Exemple 1 : N_1 = 2650106352002
Exemple 2 : N_2 = 1540454208091

Partie A. Calcul de la clé

Soit N = $\overline{a_{12}a_{11}...a_1a_0}^{10}$ le nombre formé par les 13 premiers chiffres $a_{12}a_{11}...a_1a_0$ du numéro INSEE,

1. Montrer que : $N \equiv -16 \times \overline{a_{12}a_{11}a_{10}a_9a_8}^{10} + 9 \times \overline{a_7a_6a_5a_4}^{10} + \overline{a_3a_2a_1a_0}^{10}$ [97]
2. Calculer la clé dans l'exemple ci-dessus.

Partie B. Utilité de la clé

1. Changer l'un des chiffres du nombre N donné dans l'exemple ci-dessus. La clé est-elle modifiée ?
2. Montrons que c'est toujours le cas et que la clé permet donc de détecter toute erreur faite sur un chiffre de N.
   Soit N et sa clé C. Notons N' un nombre formé en modifiant un seul des chiffres de N, et C' sa clé.
   On supposera que N > N'.

a. A quelle condition sur N et N' les clés C et C' sont-elles les mêmes?
b. Montrer que N – N' est de la forme $\alpha . 10^m$ où α et *m* sont des entiers tels que $1 \leq \alpha \leq 9$ et $0 \leq m \leq 12$.
c. Quels sont les nombres premiers qui peuvent intervenir dans la décomposition en facteurs premiers de N – N'?
d. Vérifier que 97 est premier. En déduire que 97 ne divise pas N – N'. Conclure.

Partie C. Ses limites

Donner un exemple d'erreur non détectée par la clé.

CORRECTION

Partie A. Calcul de la clé

1. $N = \overline{a_{12}a_{11}...a_1a_0}^{10} = 10^8 \times \overline{a_{12}a_{11}a_{10}a_9a_8}^{10} + 10^4 \times \overline{a_7a_6a_5a_4}^{10} + \overline{a_3a_2a_1a_0}^{10}$

$10^2 \equiv 3$ [97] donc $10^4 \equiv 9$ [97] et $10^8 \equiv 81$ [97] or 81 = 97 – 9 donc $81 \equiv -6$ [97]

donc $10^8 \times \overline{a_{12}a_{11}a_{10}a_9a_8}^{10} + 10^4 \times \overline{a_7a_6a_5a_4}^{10} + \overline{a_3a_2a_1a_0}^{10} \equiv -16 \times \overline{a_{12}a_{11}a_{10}a_9a_8}^{10} + 9 \times \overline{a_7a_6a_5a_4}^{10} + \overline{a_3a_2a_1a_0}^{10}$ [97]

2. Exemple 1 : N_1 = 2650106352002

2650106352002 = 26501 0635 2002 donc $N_1 \equiv -16 \times 26501 + 9 \times 635 + 2002$

2002 = 97 × + 62 donc 2002 ≡ 62 [97] ; et 635 = 97 × 9 + 53 donc 635 ≡ 53 [97] ; et 26501 = 97 × 273 + 20 donc 26501 ≡ 20 [97]

donc $N_1 \equiv -16 \times 20 + 9 \times 53 + 62$ [97] soit $N_1 \equiv 219$ [97]

219 = 2 × 97 + 25 donc $N_1 \equiv 25$ [97] donc la clé est C = 97 – 25 = 72

Exemple 2 : N_2 = 1540454208091

1540454208091 = 15404 5420 8091donc $N_1 \equiv -16 \times 15404 + 9 \times 5420 + 8091$

8091 = 97 × + 83 donc 8091 ≡ 83 [97] ; et 5420 = 97 × 55 + 85 donc 5420 ≡ 85 [97] ; et 15404 = 97 × 158 + 78 donc 15404 ≡ 20 [97]

donc $N_1 \equiv -16 \times 20 + 9 \times 85 + 83$ [97] soit $N_1 \equiv -443$ [97]

– 443 = – 5 × 97 + 42 donc $N_1 \equiv 42$ [97] donc la clé est C = 97 – 42 = 55

Partie B. Utilité de la clé

1. N_1 = 2650106352002 soit $N'_1 = N_1 + 1$

donc $N'_1 \equiv 25 + 1$ [97] donc la clé de N'_1 est C = 97 – 26. La clé est modifiée

2. *a*. Il existe un nombre *n* compris entre 0 et 96 tel que $N \equiv n$ [97], et un nombre *n'* compris entre 0 et 96 tel que $N' \equiv n'$ [97]

C = C' ⇔ 97 – *n* = 97 – *n'* ⇔ *n* = *n'* ⇔ N ≡ N' [97]

b. N et N' diffèrent par un seul chiffre soit a_m le chiffre de N modifié par b_m dans N'avec $0 \leq m \leq 12$

N > N' donc $a_m > b_m$ donc N – N' = $(a_m - b_m)\ 10^m$ avec $0 \leq a_m - b_m$

$0 \leq b_m \leq 12$ et $0 \leq b_m \leq 12$ donc $a_m - b_m \leq 12$ donc N – N' est de la forme $\alpha . 10^m$ où α et *m* sont des entiers tels que $1 \leq \alpha \leq 9$ et $0 \leq m \leq 12$.

c. N – N' est de la forme $\alpha . 10^m$ où α et *m* sont des entiers tels que $1 \leq \alpha \leq 9$ et $0 \leq m \leq 12$.

Les nombres premiers qui interviennent dans la décomposition en facteurs premiers de α sont 2 ; 3 ; 5 ; 7
Les nombres premiers qui interviennent dans la décomposition en facteurs premiers de 10^m sont 2 ; 5
les nombres premiers qui peuvent intervenir dans la décomposition en facteurs premiers de N – N' sont donc 2 ; 3 ; 5 ; 7.

d. 97 n'est pas divisible par 2 ; 3 ; 5 ; 7 ; 11 et $11^2 > 97$ donc 97 est un nombre premier.
La décomposition en facteur premiers de N – N' ne peut faire intervenir que 2 ; 3 ; 5 ; 7 or 97 est premier avec chacun de ces nombres donc avec leur produit donc 97 ne divise pas N – N' donc C ≠ C'

Partie C. Ses limites

N_1 = 2650106352002 et $N'_1 = N_1 + 97$ soit N'_1 = 2650106352099 alors $N_1 \equiv 25$ [97] et $N'_1 \equiv 25$ [97] donc les deux clés seront identiques, l'erreur est non détectée par la clé.