Nations Unies ECE/TRANS/SC.2/PIRRS/2020/4

Conseil économique et social

Distr. générale
13 juillet 2020
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des transports par chemin de fer

Groupe d'experts de l'identification permanente du matériel roulant ferroviaire

Première session
Genève, 2-4 septembre 2020
Point 5 de l'ordre du jour provisoire
Élaboration du Système d'individualisation des véhicules ferroviaires

Introduction à l'algorithme de Luhn

Document présenté par le Rail Working Group*

I. Introduction

1. L'algorithme de Luhn porte le nom de son créateur allemand, le chercheur en informatique Hans Peter Luhn. Il s'agit d'une simple formule de vérification des chiffres utilisée très largement pour valider les numéros d'identification. Son champ d'applications éprouvées est très vaste[1] :

- Numéros de cartes de crédit,
    - VISA, AMEX, Mastercard, Diners Club, etc. ;
- Cartes nationales américaines d'identification des prestataires de soins de santé ;
- Numéros d'assurance sociale canadiens et grecs ;
- Numéros d'identification nationaux israéliens et sud-africains ;
- Codes d'enquête figurant sur les reçus des grandes chaînes de restauration ;
    - McDonalds, Taco Bell, etc.

2. L'algorithme, qui est dans le domaine public, est détaillé dans la norme ISO/IEC 7812. Contrairement aux techniques de sécurité brevetées plus perfectionnées, l'algorithme de Luhn n'a pas pour objectif de protéger contre les pirates informatiques. C'est une méthode simple utilisée pour distinguer les numéros valides de ceux qui ne le sont pas, par exemple à cause de fautes de frappe.

* Il a été convenu que le présent document serait publié après la date normale de publication en raison de circonstances indépendantes de la volonté du soumetteur.

[1] www.geeksforgeeks.org/luhn-algorithm/.

II. Fonctionnement de l'algorithme

3. Prenons le numéro 12345674 et supposons qu'il s'agit d'un numéro de carte de crédit valide. Le dernier chiffre (4) est une sorte de clef de contrôle (également appelée chiffre d'autocontrôle) qui permet de vérifier l'intégrité des autres chiffres. Si on soumet à l'algorithme de Luhn la première partie du numéro dans laquelle deux chiffres auront été intervertis (par exemple 1324567 au lieu de 1234567), un résultat autre que 4 sera généré, révélant que le numéro n'est pas valide.

III. Détail des calculs sur lesquels sont fondés les contrôles de validité

4. L'algorithme de Luhn s'applique en commençant par le dernier chiffre du numéro, situé tout à droite, et en remontant jusqu'au premier, à gauche. Il faut multiplier par 2 tous les chiffres qui sont en position paire, en allant de gauche à droite comme indiqué précédemment. Si le double d'un chiffre est égal ou supérieur à 10, on le remplace par la somme des chiffres qui le composent. On additionne alors tous les chiffres obtenus pour avoir la somme s. Pour trouver le chiffre d'autocontrôle c, on applique la formule c = (10 − (smod10) mod10). (Rappel : mod renvoie à l'opération modulo, qui sert à calculer le reste de la division euclidienne. La calculatrice modulo renvoie le reste de la division des nombres entiers.)

IV. Utilisation de la formule[2]

5. Voici un exemple concret d'utilisation de la formule :

- On veut trouver le chiffre d'autocontrôle X dans le numéro 853X.
- On prend le chiffre 3 et on le multiplie par 2, soit 3 * 2 = 6.
- Quant au chiffre 5, on ne le multiplie pas par 2.
- On multiplie 8 par 2, soit 8 * 2 = 16. Puisque le résultat est supérieur à 10, on additionne les chiffres qui le composent, soit 1 + 6 = 7.
- La somme s correspond à 6 + 5 + 7 = 18. Étant donné que 18 mod 10 = 8, le calcul final donne :
- c = (10 – 8mod10) = (10 – 8) = 2.
- Par conséquent, 2 est le chiffre d'autocontrôle et le numéro 8532 est valable selon l'algorithme de Luhn.

Voici un tableau qui permet de mieux visualiser cet exemple :

8	*5*	*3*	*0*
8 * 2 = 16	Reste 5	3 * 2 = 6	Reste 0
1 + 6 = 7	5	6	0
s = 7	+5	+6	+0 = 18
			c = 10 – ((18mod10)mod10)
			c = 10 – (8mod10)
			c = 10 – 8
			c = 2

[2] www.dcode.fr/luhn-algorithm.

V. Conclusion

6. L'algorithme de Luhn est un moyen efficace et accessible au public de vérifier la validité des numéros d'identification. Il ne protège pas contre les attaques, n'est pas utilisé par les banques pour calculer les codes de vérification des cartes et ne permet pas non plus de contrôler la validité des dates figurant sur les cartes[3].

7. L'algorithme de Luhn détectera toute erreur concernant un seul chiffre et presque tous les cas où deux chiffres adjacents sont intervertis. Il a cependant quelques défauts :

a) Il ne détecte pas les cas où les séquences à deux chiffres 09 et 90 sont interverties, dans un sens ou dans l'autre[4] ;

b) Il détecte la plupart des cas où une séquence de deux chiffres identiques est remplacée par deux autres chiffres identiques, sauf les suivants : 22 ↔ 55, 33 ↔ 66 et 44 ↔ 77[5].

8. Des algorithmes plus complexes et plus fiables existent, comme l'algorithme de Verhoeff, mais comparativement leur utilisation commerciale est assez limitée. Ils ne sont tout simplement pas aussi pratiques (surtout du point de vue du calcul et de la gestion) que l'algorithme de Luhn, qui, comme démontré ci-dessus, peut être appliqué sans autres outils qu'un stylo et du papier et offre des solutions à toutes sortes d'émetteurs de numéros importants.

[3] www.investopedia.com/terms/l/luhn-algorithm.asp.
[4] https://planetcalc.com/2464/.
[5] Kamaku et Wachira, « Twin Error Detection in Luhn's Algorithm » (2015).