Экономический и Социальный Совет

Distr.: General
13 July 2020
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по железнодорожному транспорту

Группа экспертов по постоянной идентификации железнодорожного подвижного состава

Первая сессия
Женева, 2—4 сентября 2020 года
Пункт 5 предварительной повестки дня
Разработка Системы уникальной идентификации рельсовых транспортных средств

Общая информация об алгоритме Луна

Представлено Железнодорожной рабочей группой*

I. Введение

1. Алгоритм Луна получил название по имени своего немецкого разработчика — специалиста по информатике Ханса Петера Луна. Это простой алгоритм проверки контрольной цифры, широко используемый для проверки правильности идентификационных номеров. Область его практического применения весьма широка[1]:

- номера банковских карт,
    - в том числе карт систем VISA, AMEX, Mastercard, Diners Club и т. д.;
- национальные коды учреждений — поставщиков медицинских услуг в США;
- номера социального страхования в Канаде и Греции;
- номера национальных удостоверений личности в Израиле и Южной Африке;
- коды вопросников, размещаемые на кассовых чеках крупных ресторанных сетей,
    - включая рестораны Макдоналдс, Тако Белл и т. д.

* Настоящий документ был запланирован к изданию после установленного срока в силу обстоятельств, не зависящих от представившей его стороны.

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

2. Алгоритм является общественным достоянием и описан в стандарте ISO/IEC 7812. В отличие от более сложных коммерческих программ обеспечения безопасности, алгоритм Луна не предназначен для защиты от злонамеренных действий хакеров. Вместо этого использование алгоритма Луна позволяет легко отличить верно введенные числовые коды от числовых кодов, введенных с ошибкой, например в результате опечатки.

II. Суть алгоритма

3. Возьмем число 12345674. Предположим, что это верный номер кредитной карты. Последняя цифра «4» является своего рода контрольным ключом (или контрольной цифрой) для проверки правильности остальных цифр. Если в исходной последовательности поменять местами две цифры и применить алгоритм Луна к новой последовательности (например, 1324567 вместо 1234567), то полученный результат будет отличным от 4, что подтверждает наличие ошибки в новой последовательности.

III. Тщательный анализ алгоритма, позволяющего проверять правильность числовых последовательностей

4. В алгоритме Луна все цифры последовательности нумеруются начиная с ее конца, т. е. начиная с первой цифры, расположенной справа, и заканчивая первой цифрой, расположенной слева. Все цифры, занимающие в последовательности четные позиции (нумерация которых идет справа налево, как уже было указано выше), умножаются на 2. Если результатом умножения на 2 является число, равное или большее 10, оно заменяется суммой его цифр. После этого вычисляется сумма «s» всех полученных цифр. Контрольная цифра «c» определяется по формуле $c = (10 - (s \bmod 10)) \bmod 10$. (Напоминаем: mod означает операцию modulo. Так называют вычисление остатка в евклидовом делении. В результате операции modulo получают остаток от деления на целое число.)

IV. Пример применения алгоритма[2]

5. Ниже приводится конкретный пример использования алгоритма:

- Имеется числовая последовательность 853X, для которой необходимо вычислить контрольную цифру X.
- Берется цифра 3, которая умножается на два: 3 * 2 = 6.
- Берется цифра 5, которая не умножается на 2.
- Берется цифра 8, которая умножается на 2: 8 * 2 = 16. Поскольку полученное произведение больше 10, находится сумма его цифр: 1 + 6 = 7.
- Рассчитывается сумма s: 6 + 5 + 7 = 18. Поскольку 18 mod 10 = 8, окончательный расчет позволяет получить
- $c = (10 - 8 \bmod 10) = (10 - 8) = 2$.
- Контрольная цифра — 2. Таким образом, алгоритм Луна подтверждает правильность последовательности 8532.

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

Следующая таблица помогает разобраться с приведенным выше примером:

8	*5*	*3*	*0*
8 * 2 = 16	Остается 5	3 * 2 = 6	Остается 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

V. Заключение

6. Алгоритм Луна представляет собой эффективный и общедоступный способ проверки правильности чисел. Использование этого алгоритма не может защитить от вредоносных атак, и он не используется банками для расчета кодов проверки подлинности карты. Кроме того, алгоритм Луна не позволяет проверить правильность указываемого на картах срока годности[3].

7. Однако алгоритм Луна позволяет выявлять любые ошибки, связанные с искажением одной цифры, а также практически все парные перестановки двух идущих подряд цифр. Вместе с тем у данного алгоритма имеются определенные недостатки:

a) он не позволяет обнаружить замену двузначной последовательности 09 на 90 (или наоборот)[4];

b) он позволяет обнаружить бóльшую часть искажений двух идущих подряд цифр, за исключением замен 22 ↔ 55, 33 ↔ 66 или 44 ↔ 77)[5].

8. Существуют более сложные и более надежные алгоритмы (например, алгоритм Верхуффа), однако возможности для их коммерческого использования сравнительно ограничены. С точки зрения удобства применения (особенно для вычисления и управления) они уступают алгоритму Луна, для использования которого, как отмечалось выше, достаточно лишь ручки и бумаги и который позволяет найти подходящее решение для всевозможных организаций, в которых генерируются длинные числовые последовательности.

[3] www.investopedia.com/terms/l/luhn-algorithm.asp.

[4] https://planetcalc.com/2464/.

[5] Kamaku and Wachira, Twin Error Detection in Luhn’s Algorithm (2015).