**Faculdade de Engenharia da Universidade do Porto**



Copa dos Libertadores da América

Base de Dados

**Licenciatura em Engenharia Informática e Computação- 2021-2022**

**Turma 2LEIC06**

**Grupo 9**

Estudantes & Autores:

João Miguel da Silva Lourenço up202108863@fe.up.pt

Tiago Ribeiro de Sá Cruz [up202108810@fe.up.pt](mailto:up202108810@fe.up.pt)

Tomás Filipe Fernandes Xavier up202108759@fe.up.pt

Resumo

Um algoritmo de verificação de números tem o propósito de garantir que determinada série de dígitos transmitida a um recetor é válida e autêntica. Com uma aplicação em massa desde o século passado é, neste momento, imprescindível a uma fácil e correta transmissão de dados. Intrinsecamente inserido no quotidiano do cidadão comum, mas facilmente despercebido, é utilizado em diversas áreas como a banca, logística e entidades governamentais utilizando diferentes operações aritméticas para efetuar a validação do dígito de controlo. Neste relatório é feita uma análise à história dos algoritmos de verificação, uma breve introdução aos conceitos de aritmética modular, o estudo das aplicações contemporâneas e uma análise aos seus respetivos exemplos.

Palavras-Chave

Dígito verificador, Módulo 10, Módulo 11, Aritmética Modular, ISBN, IMEI, Algoritmo de Luhn, IBAN, EAN, Transmissão de Dados.

Índice

[Lista de figuras iv](#_heading=h.57e57l1joibu)

[Lista de tabelas iv](#_heading=h.1ksv4uv)

[Lista de acrónimos v](#_heading=h.3whwml4)

[1. Introdução 1](#_heading=h.2bn6wsx)

[2. Aritmética Modular 2](#_heading=h.qsh70q)

[2.1 Noções Elementares 2](#_heading=h.3as4poj)

[2.2 Algoritmo de verificação de números 2](#_heading=h.cbkjo8gu4hqb)

[3. Evolução dos algoritmos de verificação de números 3](#_heading=h.llurhsxt8vud)

[4. Aplicações 4](#_heading=h.np8v0h85espa)

[4.1 Sistema EAN-UCC 4](#_heading=h.49x2ik5)

[4.1.1 Cálculo do Dígito de Controlo EAN-UCC 4](#_heading=h.147n2zr)

[4.2 Sistema de Identificação do Cartão de Cidadão 5](#_heading=h.nms404t6di1a)

[4.2.1 Validação do Número de Documento. 6](#_heading=h.1hmsyys)

[4.3 Sistema ISBN 7](#_heading=h.2grqrue)

[4.3.1 Cálculo do Dígito de Verificação do ISBN 7](#_heading=h.vx1227)

[4.4 Sistema IMEI 8](#_heading=h.1v1yuxt)

[4.5 Sistema IBAN 9](#_heading=h.2u6wntf)

[4.5.1 Validação do IBAN 9](#_heading=h.3tbugp1)

[4.6 Aplicações na comunidade FEUP 10](#_heading=h.nmf14n)

[4. Conclusões 11](#_heading=h.37m2jsg)

[Referências bibliográficas 12](#_heading=h.1mrcu09)

[Apêndices 13](#_heading=h.46r0co2)

# Lista de figuras

[Figura 1 - Relógio Modular (Academy) 2](#_heading=h.1pxezwc)

[Figura 2 - Exemplos de Códigos EAN (CODIPOR 2016) 4](#_heading=h.2p2csry)

[Figura 3 - Cartão de Cidadão genérico (Portimão 2021) 6](#_heading=h.32hioqz)

[Figura 4 - Caracterização de um IBAN. 9](#_heading=h.19c6y18)

# Lista de tabelas

[Tabela 1 – Resumo do cálculo do dígito de verificação. Adaptado de (CODIPOR 2016). 5](#_heading=h.3o7alnk)

[Tabela 2 – Exemplo de cálculo do dígito de verificação de um código EAN-8 (CODIPOR 2016). 5](#_heading=h.23ckvvd)

[Tabela 3 – Validação de um número de documento de um cartão de cidadão genérico (Admnistrativa 2009). 6](#_heading=h.41mghml)

[Tabela 4 - Validação do ISBN de um livro (Agency 2017). 8](#_heading=h.3fwokq0)

[Tabela 5 - Cálculo do dígito de controlo de um IMEI. 9](#_heading=h.4f1mdlm)

[Tabela 6 - Validação de um IBAN genérico 10](#_heading=h.28h4qwu)

[Tabela 7 - Conversão de letras em valores numéricos. 13](#_heading=h.2lwamvv)

# Lista de acrónimos

EAN – European Article Number

FEUP – Faculdade de Engenharia da Universidade do Porto

GSMA – Global System for Mobile Communications

IBM – International Business Machines

IBAN – International Bank Account Number

IMEI – International Mobile Equipment Identity

ISBN – International Standard Book Number

TAC – Type Allocation Code

UCC – Universal Comercial Code

UPC – Universal Product Code

# 1. Introdução

Desde há muitos anos, a identificação de objetos, serviços e locais é feita através de uma atribuição de um conjunto de dígitos organizados com um tamanho de ordem fixa. A sua autenticidade pode ser verificada através da atribuição de um processo de controlo sobre esse número. Geralmente esse processo depende de um valor introduzido por um humano, o que é suscetível à ocorrência de erros ou à tentativa de fraude. Por exemplo, ao inserir manualmente um código de barras de um produto de supermercado numa caixa registadora, existe a possibilidade do operador inserir um conjunto de dígitos de tamanho diferente ao suposto, e de colocar os dígitos por uma ordem errada. O erro humano constitui assim um grande fator na transmissão errada de dados.

Com a internacionalização de operações e partilha de dados global surge a necessidade de garantir que a transmissão de um emissor para um recetor é fidedigna. Para impedir a transmissão de dados errados são utilizadas técnicas de aritmética modular que fazem a validação do número de identificação. Este relatório, realizado no âmbito da unidade curricular “Projeto FEUP”, focar-se-á particularmente no algoritmo de verificação de números, sendo efetuada a pesquisa sobre o seu aparecimento, as técnicas utilizadas e as aplicações contemporâneas.

# 

# 2. Aritmética Modular

## 2.1 Noções Elementares

A aritmética modular consiste em operações que utilizam o resto da divisão de números inteiros. O número obtido do resto de um determinado dividendo designa-se pelo módulo do divisor utilizado. Por exemplo ao dividir-se “10” por “3”, o número inteiro que se obtém no quociente é “3”, multiplicando pelo divisor, obtém-se “9”, ao que se tem de somar “1” (resto) para se obter o dividendo original (Santos, 2013).

Um exemplo prático para visualizar mais facilmente este cálculo é o exemplo do relógio (Academy). Um relógio tem 12 dígitos, se se imaginar um relógio que começa em 0 e vai até 11, pode-se calcular o módulo 12 de qualquer número contando a quantidade de vezes que se tem de mover. Mas atenção, é necessário ter em conta se o dividendo é um número inteiro positivo ou negativo. Tome-se o exemplo do inteiro positivo “3”. Não é possível multiplicar nenhum número por “12” e obter-se “3”, logo tem que se ir ao relógio e ver o módulo 12 deste número. Verifica-se que se move 3 vezes que é equivalente ao módulo que se procurava.

Uma imagem com texto, relógio

Descrição gerada automaticamente

*Figura 1 - Relógio Modular (Academy)*

## 2.2 Algoritmo de verificação de números

Um algoritmo de verificação de números é, como qualquer outro algoritmo, uma sequência de passos que são executados para resolver determinado problema e que depende também dos dados fornecidos (“*input*”). O objetivo deste é criar um número denominado de dígito de verificação (“*check digit*”) a partir da sequência de números fornecida.

O dígito de verificação ou algarismo de controlo é assim usado para testar a validade e autenticidade do valor introduzido, evitando, desta forma, fraudes ou erros de transmissão, leitura ou digitação. Em alguns algoritmos, sãos criados, não um, mas vários algarismos de controlo, variando assim a sua complexidade

Existem vários tipos de algoritmos diferentes para este problema, sendo alguns mais complexos ou simples, antigos ou recentes. Alguns exemplos mais conhecidos serão dados nos tópicos seguintes, explicando-se o mecanismo e a aplicação destes tais algoritmos.

# 3. Evolução dos algoritmos de verificação de números

Os algoritmos de verificação não são uma invenção muito antiga, mas, apesar disso, detêm uma certa história. A sua primeira versão tem o nome de *“Luhn Algorithm”,* ou Módulo 10, este nome foi dado em honra do seu criador, o cientista de computadores alemão *Hans* *Peter Luhn* que desenvolveu o algoritmo em 1954 durante os seus dias como investigador na empresa IBM. Esta sua forma utiliza aritmética modular, criada por Carl Friedrich Gauss durante o século XIX (Cardless).

O algoritmo de Luhn baseia-se numa série de operações matemáticas que, caso o número total acabe num zero (e.g. 70) então o número é válido. Este algoritmo ainda é muito usado atualmente para validar números de identificação de cartões de crédito. Apesar disso, o Módulo 10 foi desenhado para proteger contra erros acidentais e não para ser usado como proteção contra ataques maliciosos (Gupta).

Já em 1969, foi desenvolvido o *“Verhoeff algorithm”* pelo matemático holandês *Jacobus Verhoeff* que, tal como o algoritmo de Luhn, verifica a validade do número introduzido através de uma série de cálculos, mas, mostrou-se com avanços significativos que permitia que fosse possível detetar todos os erros de um único dígito e todos os erros que envolviam dois dígitos adjacentes (Algorithms).

Por fim e mais recentemente, em 2004, *H. Michael Damm* desenvolveu o *“Damm Algorithm”*, que escreveu na sua tese de doutoramento. Este seu algoritmo é bastante parecido ao de Verhoeff, mas, por sua vez, apenas utiliza os números de 0 a 9 e deteta todos os erros singulares e de transposição de algarismos adjacentes, sendo assim bem mais simples e detetando também erros de transcrição devido a uma pronúncia parecida, tal como o 15 e 50, do inglês *“fifteen”* e *“fifty”* (Teixeira, 2015).

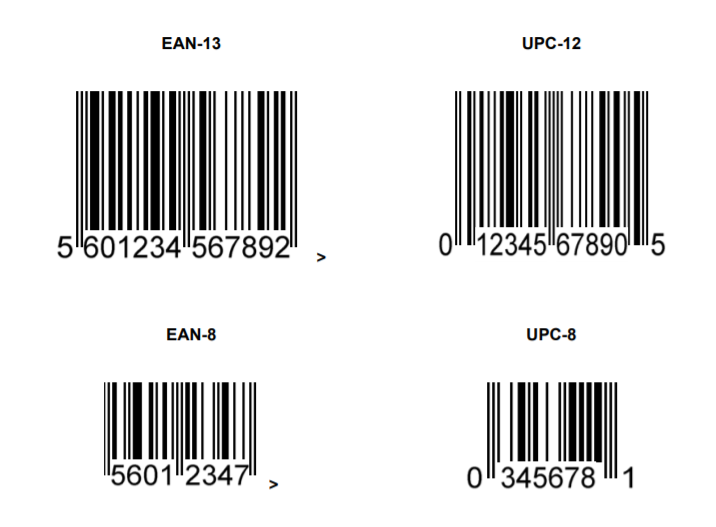
# 4. Aplicações

## 4.1 Sistema EAN-UCC

O sistema EAN-UCC *– European Article Number-Universal Comercial Code,* utiliza um conjunto de números em forma de código de barras para a identificação e codificação de unidades comerciais, unidades logísticas, ativos e localizações.

A identificação numérica utilizada é a chave de acesso às bases de dados inseridas nos sistemas informáticos de quem faz a leitura do código. Esta permite ao utilizador obter toda informação que descreve o produto/serviço.

Na Figura 2 observa-se vários exemplos de códigos de barras utilizados para transmissão de informação em pontos de venda. O código pode ser lido omnidireccionalmente e o seu último dígito é o de controlo.



*Figura 2 - Exemplos de Códigos EAN (CODIPOR, 2016)*

### 4.1.1 Cálculo do Dígito de Controlo EAN-UCC

De acordo com a posição dos dígitos no código de barras é atribuída uma constante que é multiplicada pelo dígito de posição “N”. Neste caso específico intercala-se a multiplicação de cada dígito por “3” e por “1”, diferindo a ordem de utilização de acordo com o código. Soma-se o resultado das multiplicações e subtrai-se ao múltiplo de 10 mais próximo. A diferença entre esses dois números corresponderá ao dígito de verificação.

Na Tabela 1 estão expostos os dados necessários para o cálculo dos exemplos de código de barras demonstrados na Figura 2.

*Tabela 1 – Resumo do cálculo do dígito de verificação. Adaptado de (CODIPOR, 2016).*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Posição dos Dígitos | | | | | | | | | | | | *Check Digit* |
| EAN-13 | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 | N9 | N10 | N11 | N12 | N13 |
| EAN-8 | - | - | - | - | - | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 |
| UPC-12 | - | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 | N9 | N10 | N11 | N12 |
| UPC-8 | - | - | - | - | - | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 |
| Constante | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | - |

Pegando no código EAN-8 da Figura 2 tem-se o seguinte número “56012347” sendo o dígito “7” o de verificação. Na Tabela 2 demonstra-se os passos necessário para o seu cálculo. Calculando a soma acumulada de cada dígito obtém-se “43”. O múltiplo de “10” superior a esse número mais próximo é “50”, que ao subtrair por “43” dá “7”, o dígito de verificação correto exposto no exemplo.

*Tabela 2 – Exemplo de cálculo do dígito de verificação de um código EAN-8 (CODIPOR, 2016).*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Dígitos por posição | | | | | | | *Check Digit* |
| EAN-8 | 5 | 6 | 0 | 1 | 2 | 3 | 4 | 7 |
| Constante | x3 | x1 | x3 | x1 | x3 | x1 | x3 | Resultado |
| Resultado | 15 | 6 | 0 | 1 | 6 | 3 | 12 | 43 |
| Múltiplo de 10 | 50 | | | | | | | - |
| Diferença | 50-43 | | | | | | | 7 |

## 4.2 Sistema de Identificação do Cartão de Cidadão

O cartão de cidadão é um bom exemplo da utilização de um digito de verificação de elevada complexidade. O número de documento é composto por um número de identificação de oito dígitos, um digito de verificação desse número, pela versão desse cartão que pode ser um dígito ou letra e por um digito de verificação do número de documento. Resumidamente apresenta-se no seguinte formato:

DDDDDDDD C AAT

Em que:

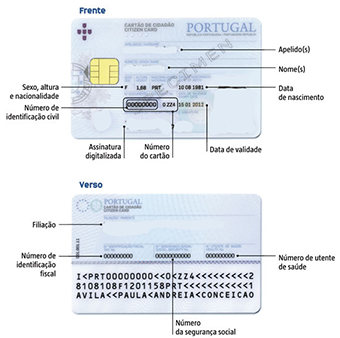
D – Número de identificação cívil [0…9]

C – Dígito de verificação do número de identificação cívil [0...9]

A – Versão [A...Z, 0…9]

T – Dígito de verificação do número de documento [0…9]

Na Figura 3 observa-se um exemplo de um cartão de cidadão genérico legendado.



*Figura 3 - Cartão de Cidadão genérico (Portimão, 2021)*

### 4.2.1 Validação do Número de Documento.

A validação do documento é feita através de operações matemáticas e modulares sobre o número completo do documento. Também existem condicionantes nos resultados dessas operações que interferem no resultado da validação.

O processo, (Admnistrativa, 2009), é feito da seguinte forma:

* Começando da direita para a esquerda duplica-se o dígito a cada segundo elemento lido. Se algum dos caracteres é uma letra esta tem de ser substituída pelo número correspondente pré-estabelecido (ver apêndice A).
* Se o resultado desta duplicação for superior a “10” tem que se subtrair ao seu valor “9”.
* Soma-se todos os valores calculados e não calculados até esta fase do processo.
* Ao resultado total aplica-se o módulo de “10”, que se for diferente de “0”, significa que o documento não é válido.

Aplicando a fórmula de validação a um número de identificação genérico da Figura 3 observa-se os resultados da Tabela 3 e a sua respetiva validade.

*Tabela 3 – Validação de um número de documento de um cartão de cidadão genérico (Admnistrativa, 2009).*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operação | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Z (35) | Z (35) | 4 |
| Duplicação | 0 | - | 0 | - | 0 | - | 0 | - | 0 | - | 70 | - |
| Subtração por 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 35 | 61 | 4 |
| Soma | 100 | | | | | | | | | | | |
| Módulo de 10 | 0 | | | | | | | | | | | |

## 4.3 Sistema ISBN

O sistema ISBN – *International Standard Bool Number* é um número único de treze dígitos (até 2007 utilizava apenas sete dígitos) que identifica uma obra ou edição de uma publicação feita por determinada editora e autor num determinado formato. Utilizado em quase todos os países do planeta surge pela primeira vez em 1967 no Reino Unido pela empresa ***J Whitakers & Sons***, depois de ter sido debatido no ano transato, na Terceira Conferência Internacional de Pesquisa de Mercado do Livro e Racionalização do Comércio de Livros em Berlim, a necessidade de arranjar uma forma de controlar inventário e processar ordens de compra através de uma identificação (Agency, 2017).

Este número de identificação é subdividido em cinco elementos da seguinte forma:

1. Elemento GS1 – é um conjunto de três dígitos que indica o tipo de publicação. Estes são determinados por uma entidade pública de nome GS1 que determina padrões internacionais para comunicação empresarial (Agency, 2017).
2. Identificador de grupo – Conjunto de dígitos que variam até um limite de cinco e que indicam a região geográfica, país ou língua do sistema ISBN.
3. Código de editor – Conjunto de dígitos até um limite de sete que identifica o editor da publicação.
4. Número da publicação – Identifica a obra publicada por um determinado editor. Pode conter até seis dígitos.
5. Dígito de verificação – É o dígito que se deve obter quando utilizado um algoritmo de módulo 10 determinado pela agência internacional ISBN.

### 4.3.1 Cálculo do Dígito de Verificação do ISBN

Á semelhança do algoritmo utilizado na validação do número de identificação de um cartão de cidadão, a validação do ISBN é feita também através de operações matemáticas e modulares que envolvem a multiplicação dos dígitos pelas constantes “1” e “3” e o módulo de 10 de determinados resultados.

O algoritmo tem a seguinte sequência:

* Os doze primeiros dígitos são é multiplicado por “1” e por “3” de forma alternada respetivamente da esquerda para a direita.
* É feita a soma dos resultados da multiplicação.
* Calcula-se o módulo de 10 do resultado da soma.
* Faz-se a diferença entre 10 e o resultado obtido anteriormente, se o módulo obtido for igual a 10 então o dígito, consequentemente, será igual a 0.

Usando o ISBN “978-0-141-39543-2” de uma obra escrita por *George Orwell* com o título de *“The Burmese Days”* observa-se na Tabela 4 o cálculo do dígito de verificação que é “2”.

*Tabela 4 - Validação do ISBN de um livro (Agency, 2017).*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | GS1 | | | Ident. de grupo | Cód. de editor | | | Nº da publicação | | | | | *Check digit* | Soma |
| ISBN | 9 | 7 | 8 | 0 | 1 | 4 | 1 | 3 | 9 | 5 | 4 | 3 | 2 | - |
| Constante | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | x1 | x3 | - | - |
| Produto | 9 | 21 | 8 | 0 | 1 | 12 | 1 | 9 | 9 | 15 | 4 | 9 | - | 98 |
| Módulo 10 | 8 | | | | | | | | | | | | | |
| Diferença | 10 - 8 = 2 | | | | | | | | | | | | | |

## 4.4 Sistema IMEI

O IMEI – International Mobile Equipment Identity, é um número único, com quinze dígitos, que identifica um dispositivo móvel. Este sistema é um exemplo das aplicações contemporâneas que utilizam o algoritmo de Luhn para calcular o dígito de controlo.

A estrutura do IMEI é descrita da seguinte forma “AA-BBBBBB-CCCCCC-D”, em que:

* AA são os dígitos de identificação do grupo do país, indicando a organização aprovada pela GSMA – Global System for Mobile Communications Association que alocou o TAC – Type Allocation Code.
* BBBBBB são os restantes dígitos do TAC.
* CCCCCC são o número de sério do modelo do dispositivo.
* D é o dígito de verificação.

A fórmula da validação do IMEI é feita da seguinte forma:

* Da direita para a esquerda duplica-se cada dígito intercaladamente.
* Soma-se todos os dígitos existentes. Ter atenção que não se somam números, se o resultado da duplicação for superior a dez, e.g. “12”, soma-se “1” e “2”.
* Subtrai-se o resultado da soma ao múltiplo de “10” imediatamente superior ao resultado e obtém-se o dígito de controlo.

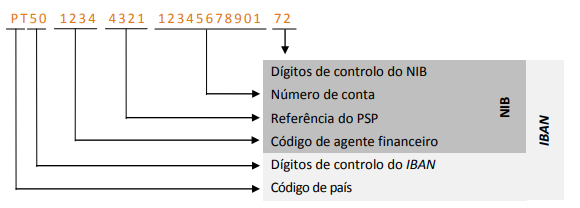
Utilizando o IMEI de um modelo de um dispositivo móvel da *Xiaomi*, “86-508605-797822-6”, observa-se na Tabela 5 o processo do cálculo do seu dígito de controlo.

*Tabela 5 - Cálculo do dígito de controlo de um IMEI.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IMEI | 8 | 6 | 5 | 0 | 8 | 6 | 0 | 5 | 7 | 9 | 7 | 8 | 2 | 2 | 6 |
| Dobro | 8 | 12 | 5 | 0 | 8 | 12 | 0 | 10 | 7 | 18 | 7 | 16 | 2 | 4 | - |
| Soma | 8+1+2+5+0+8+1+2+0+1+0+7+1+8+7+1+6+2+4 = 64 | | | | | | | | | | | | | |
| Múltiplo de 10 | 70 | | | | | | | | | | | | | |
| Diferença | 70 – 64 = 6 | | | | | | | | | | | | | |

## 4.5 Sistema IBAN

Um caso de aplicação do dígito de controlo, bem intrínseco no quotidiano do cidadão comum, é o IBAN – *International Bank Account Number*. Este número, composto por 25 caracteres alfanuméricos, identifica uma conta bancária única, associada a um cidadão, em qualquer parte do mundo. Na Figura 4 observa-se um exemplo de número IBAN onde os dois últimos dígitos são o de controlo (Portugal, 2014).



*Figura 4 - Caracterização de um IBAN.*

### 4.5.1 Validação do IBAN

O dígito de controlo é calculado utilizando por base o algoritmo de MOD-97-10. O processo de cálculo caracteriza-se da seguinte forma:

* Move-se os primeiros quatro caracteres referentes ao código de país para a direita do número.
* Converte-se as letras em valores numéricos de acordo com a Tabela 6 do apêndice A.
* Divide-se o número obtido por “97”, se o resto da divisão for igual a “1” então o número IBAN é válido.

Na Tabela 6 observa-se o exemplo da validação de um IBAN genérico.

*Tabela 6 - Validação de um IBAN genérico*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IBAN | P | T | 5 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 9 | 4 |
| Mov. | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 9 | 4 | P | T | 5 | 0 |
| Conv. | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 9 | 4 | 25 | 29 | 5 | 0 |
| ÷ 97 | 0001000012345678901942529 ÷ 97 = 1 | | | | | | | | | | | | | | | | | | | | | | | | |

## 4.6 Aplicações na comunidade FEUP

Todos os colaboradores docentes, não docentes e estudantes têm um número de identificação único. O acesso às plataformas online da comunidade utiliza este tipo de processos para verificar que o número inserido é válido.

A biblioteca da FEUP tem à disposição livros que estão devidamente identificados com um ISBN, número único para cada livro. No sistema informático estão todos os dados relativos a todas obras disponíveis à comunidade, a qual se pode ter acesso através da leitura de um código de barras. Quando alguém requisita ou devolve um livro, a entrada ou saída do sistema, identifica exatamente o livro em questão.

Também quem pretende usar os serviços da biblioteca tem que usar o seu cartão UP – Universidade do Porto, para se identificar. Neste é possível observar um conjunto de números único a cada utilizador, que é atribuído pelo emissor e mune-se também de um dígito de verificação calculado através do algoritmo de Luhn.

# 5. Conclusões

Algoritmos de verificação são utilizados em operações que são necessárias fazer validação de um número de série de identificação que é associado a um produto/serviço único. Consistem em fazer operações aritméticas aos dígitos pertencentes ao número de identificação, que de acordo com o algoritmo utilizado, verifica a autenticidade do número.

Começam a ser utilizados na metade do século passado para a identificação de obras publicadas e em meio século ganham um papel preponderante no comércio internacional e na comunicação de dados.

Apesar da sua grande importância no quotidiano, e ao contrário do que se pensa, estes algoritmos não são utilizados para cibersegurança, mas sim apenas para impedir erros de transmissão de dados.

São utilizados em diversas áreas como a logística para a identificação de produtos, banca para a identificação do número de conta, todo o tipo de indústria que utilize um número de identificação para colaboradores, indústria da produção no número de série que identifica o produto produzido, entre várias outras aplicações.

São bastante fáceis de aplicar e o seu uso constitui uma grande facilidade de comunicação entre entidades e uma maior fluidez nos canais de distribuição.

A complexidade dos algoritmos varia de acordo com a especificidade do número de série. Conclui-se que para um universo com um grande número de coisas geralmente tem um número de identificação de maior tamanho. Enquanto, que para fazer a autenticação de informação mais delicada, como o número de identificação do cartão de cidadão, o algoritmo é mais complexo.

# Referências bibliográficas

Academy, K. Aritmética Modular. Retrieved from <https://pt.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic>

Admnistrativa, A. p. a. M. (2009). *Validação de Número de Documento do Cartão de cidadão*. AMA - Agência para a Modernização Admnistrativa Retrieved from <https://www.autenticacao.gov.pt/documents/20126/115760/Valida%C3%A7%C3%A3o+de+N%C3%BAmero+de+Documento+do+Cart%C3%A3o+de+Cidad%C3%A3o.pdf>

Agency, I. I. (2017). *ISBN Users' Manual* [7ª]. Retrieved from <https://www.isbn-international.org/content/isbn-users-manual/29>

Algorithms, P. Verhoeff Algorithm. Retrieved from <https://www.programmingalgorithms.com/algorithm/verhoeff-algorithm/>

Cardless, G. What is the Luhn Algorithm? Retrieved from <https://gocardless.com/en-us/guides/posts/what-is-luhn-algorithm/>

CODIPOR, G. P. (2016). *Manual do Utilizador EAN-UCC*. Retrieved from <https://www.gs1pt.org/wp-content/uploads/2016/04/manual-utilizador-ean-ucc-72006.pdf>

Gupta, V. K. Luhn Algorithm. Retrieved from <https://www.geeksforgeeks.org/luhn-algorithm/>

Portimão, C. M. d. (2021). Cartão de Cidadão. Retrieved from <https://www.cm-portimao.pt/menus/cidadaos/criancas-e-jovens/dicas-uteis/cartao-de-cidadao>

Portugal, B. d. (2014). INTERNATIONAL BANK ACCOUNT NUMBER. *Especificações e procedimentos de validação*. Retrieved from bportugal.pt/sites/default/files/anexos/documentos-relacionados/international\_bank\_account\_number\_pt.pdf

Santos, C. F. R. S. (2013). *Aritmética Modular e suas aplicações: Dos sistemas de identificação às mensagens secretas.* (Mestre). Universidade de Coimbra, Retrieved from <https://eg.uc.pt/bitstream/10316/33700/1/Aritmetica%20modular%20e%20suas%20aplicacoes%2C%20dos%20sistemas%20de%20identificacao..._ClaudiaSeabraSantos.pdf>

Teixeira, R. E. C. (2015). *O algoritmo de Damm*. Retrieved from <http://hdl.handle.net/10400.3/3388>

# Apêndices

Apêndice A

*Tabela 7 - Conversão de letras em valores numéricos.*

|  |  |
| --- | --- |
| Letra | Valor |
| A | 10 |
| B | 11 |
| C | 12 |
| D | 13 |
| E | 14 |
| F | 15 |
| G | 16 |
| H | 17 |
| I | 18 |
| J | 19 |
| K | 20 |
| L | 21 |
| M | 22 |
| N | 23 |
| O | 24 |
| P | 25 |
| Q | 26 |
| R | 27 |
| S | 28 |
| T | 29 |
| U | 30 |
| V | 31 |
| W | 32 |
| X | 33 |
| Y | 34 |
| Z | 35 |