DIGITAL SIGNATURE

Tráfego de Informações

KEY

$$A \bmod B$$

$$\Vert$$

$$(A \pm n \cdot B) \bmod B$$

$$K_a \times K_b$$

Aritmética Modular

6.0 Propriedades do Operador Divisivo mod

A mod B

Percepto da Multiplicação, Primum

$$(a \circ b) \bmod c = [(a \bmod c) \circ (b \bmod c)] \bmod c$$

X

Percepto da Exponenciação, Secundum

$$a^{b \dot{+} d} \bmod c = [(a^{b} \bmod c) \circ (a^{d} \bmod c)] \bmod c$$

X

Percepto da Soma, Tertium

$$(a \dot{+} b) \bmod c = [(a \bmod c) \dot{+} (b \bmod c)] \bmod c$$

X

Percepto da Subtração, Quartum

$$(a \dot{-} b) \bmod c = [(a \bmod c) \dot{-} (b \bmod c)] \bmod c$$

X

Percepto da Multiplicidade, Quintum

$$a \bmod b = [(a \dot{\pm} n \circ b) \bmod b$$

Unidades de Sentido

3.0 Aplicação do Luhn Algorithm Mod 10

(MOD/U.S. PATENT No. 2950048/6-01-1954)

McDonald and Taco Bell

31287462

Documento Incompleto

	3	1	2	8	7	4	6	2
X	1	2	1	2	1	2	1	2
∑	3	2	2	7	7	8	6	4

$$\sum(3+2+2+7+7+8+6+4)=39$$

$$39 \bmod 10 = 9$$

$$\text{Complemento: } 10-9=1$$

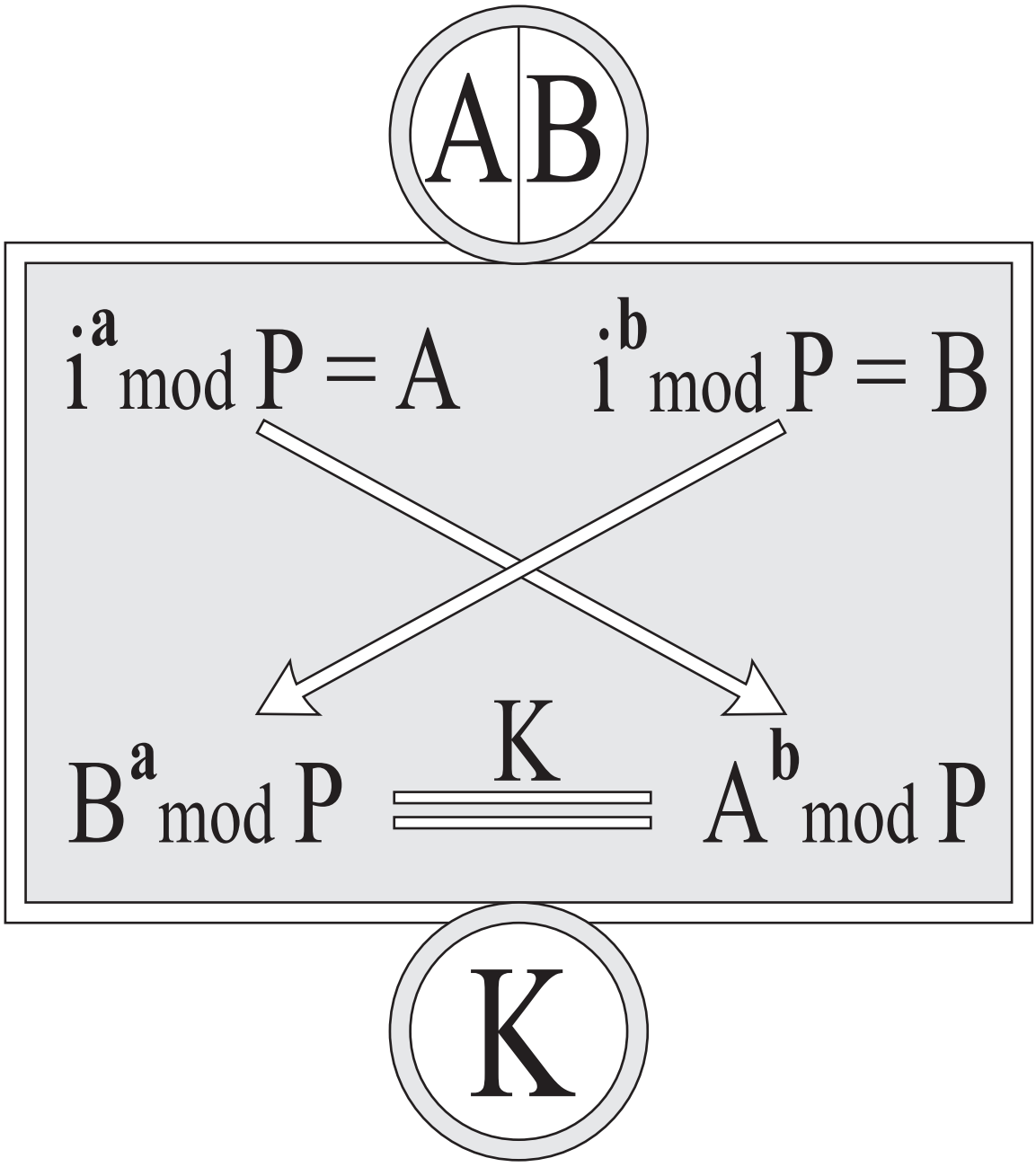
31287462 - 1

Documento Completo

Hans Peter Luhn (1896 - 1964)

DIFFIE-HELLMAN

Public Key



Private Key

Whitfield Diffie - 1976 - Martin Hellman

MENSAGEM: PRANDIANO

Pré-Codificação: 15 - 17 - 00 - 13 - 03 - 08 - 00 - 13 - 14

Codificação: (PC ✙ K)mod 26 = CD

K 16

CD (15) = (**15** ✙ 16)mod26 = **05**
CD (17) = (**17** ✙ 16)mod26 = **07**
CD (00) = (**00** ✙ 16)mod26 = **16**
CD (13) = (**13** ✙ 16)mod26 = **03**
CD (03) = (**03** ✙ 16)mod26 = **19**
CD (08) = (**08** ✙ 16)mod26 = **24**
CD (00) = (**00** ✙ 16)mod26 = **16**
CD (13) = (**13** ✙ 16)mod26 = **03**
CD (14) = (**14** ✙ 16)mod26 = **04**

05 - 17 - 16 - 03 - 19 - 24 - 16 - 03 - 04

Codificação Numérica da Palavra: Prandiano

Decodificação: (CD ▭ K)mod 26 = DC

DC(05) = (**05** ▭ 16)mod26 = (▭ 11 ✙ 26)mod26 = **15**
DC(07) = (**07** ▭ 16)mod26 = (▭ 09 ✙ 26)mod26 = **17**
DC(16) = (**16** ▭ 16)mod26 = (00 ✙ 26)mod26 = **00**
DC(03) = (**03** ▭ 16)mod26 = (▭ 13 ✙ 26)mod26 = **13**
DC(19) = (**19** ▭ 16)mod26 = (✙ 03 ✙ 26)mod26 = **03**
DC(24) = (**24** ▭ 16)mod26 = (✙ 08 ✙ 26)mod26 = **08**
DC(16) = (**16** ▭ 16)mod26 = (00 ✙ 26)mod26 = **00**
DC(03) = (**03** ▭ 16)mod26 = (▭ 13 ✙ 26)mod26 = **13**
DC(04) = (**04** ▭ 16)mod26 = (▭ 12 ✙ 26)mod26 = **14**

15 - 17 - 00 - 13 - 03 - 08 - 00 - 13 - 14

Decodificação Numérica da Palavra: Prandiano