



Função Hash

Tabela de Dispersão

X

$$h(x, k) = (h(x) + k) \bmod m$$

K

Irreversible Calculation

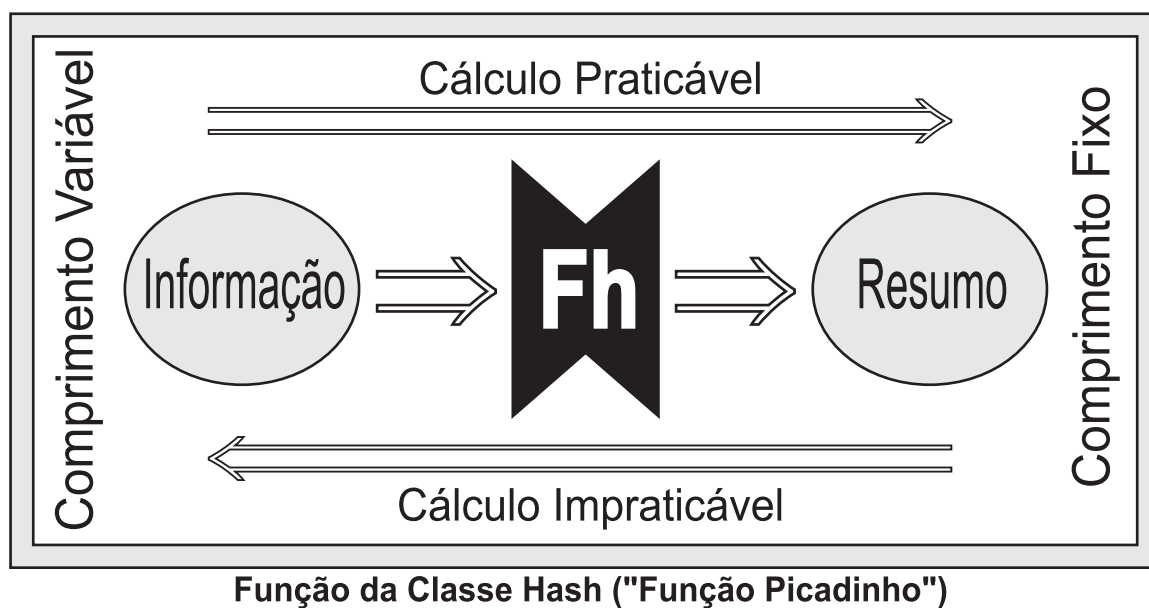


Hash Function

1.0 Formatação da Função de Classe Hash

Blockchain, grosso modo, significa registrar, codificar e distribuir publicamente informações com transparência administrativa, rapidez e invariância. Foi essa tecnologia da era do Big Data que permitiu a criação da moeda digital Bitcoin; ativo que dispensa a dependência de terceiros nas transações entre esse e aquele e aquele e um outro.

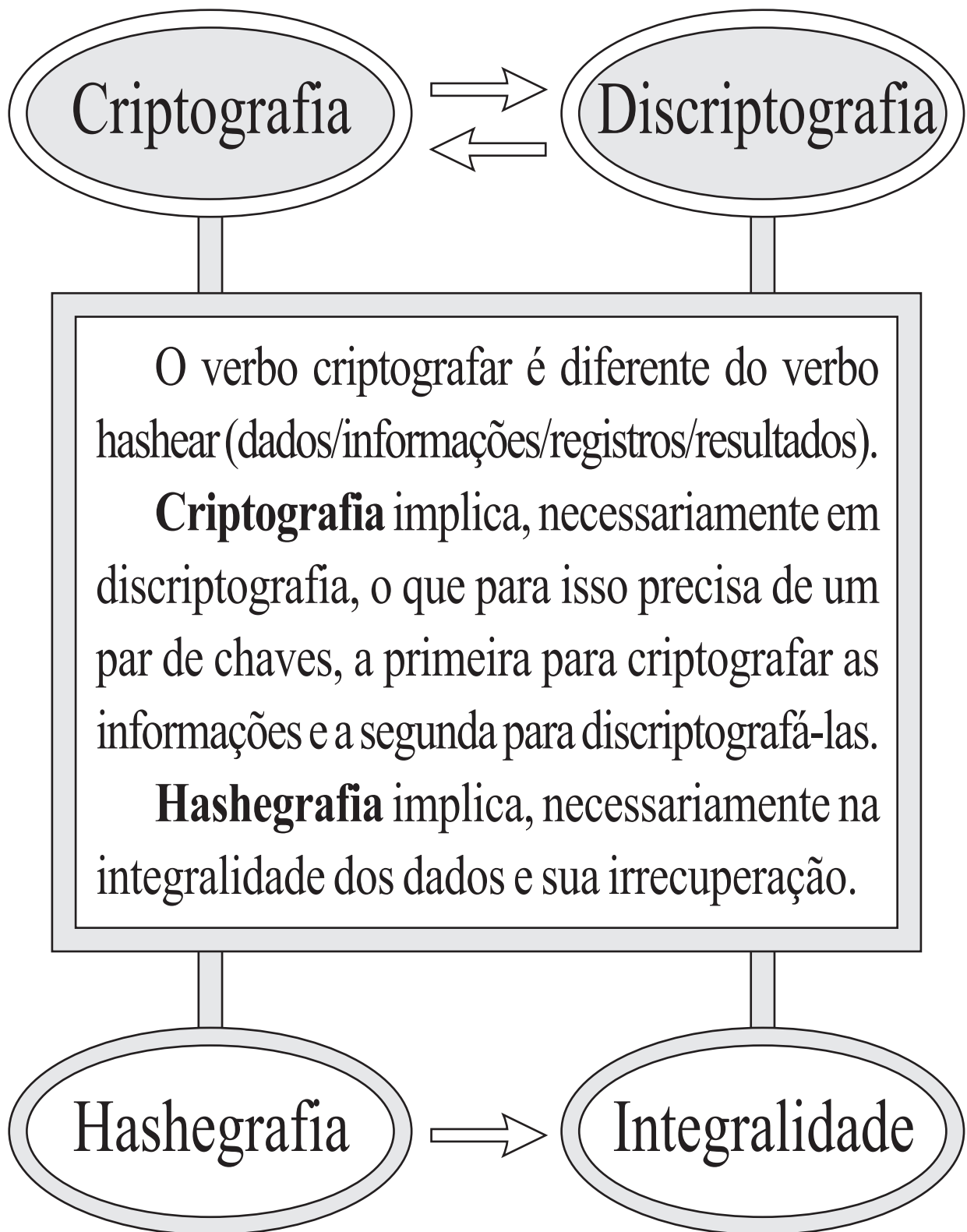
Por permitir que o registro de uma informação hasheada (Função Hash) seja rastreável em toda a sua cadeia de existência, o uso do Blockchain implica em uma certificação matemática ideal (Cartório Digital Descentralizado).



Na codificação da classe hash (rotula-se FH) qualquer alteração, mínima que seja, na informação que transita pela rede de computadores mundial, produz uma alteração no seu resumo anterior (original) de modo que os dois resumos sejam incorrelacionáveis. Esse fato permite a tão importante e desejada segurança/garantia no universo digital.



2.1 Reversibilidade X Irreversibilidade



Criptografia X Hashegrafia



2.2 Procedimento Computacional Bidirecional

Número Decimal Trafegado

$$x = 190166$$

$$x \quad f(x) = \frac{2x^2 + 8}{2} \quad f(x)$$

$$f(x) = 3616310756 \times 10^{10}$$

$$f(x) \quad x = f(x)^{-1} = \sqrt{\frac{2f(x) - 8}{2}} \quad x$$

$$x = 190166$$

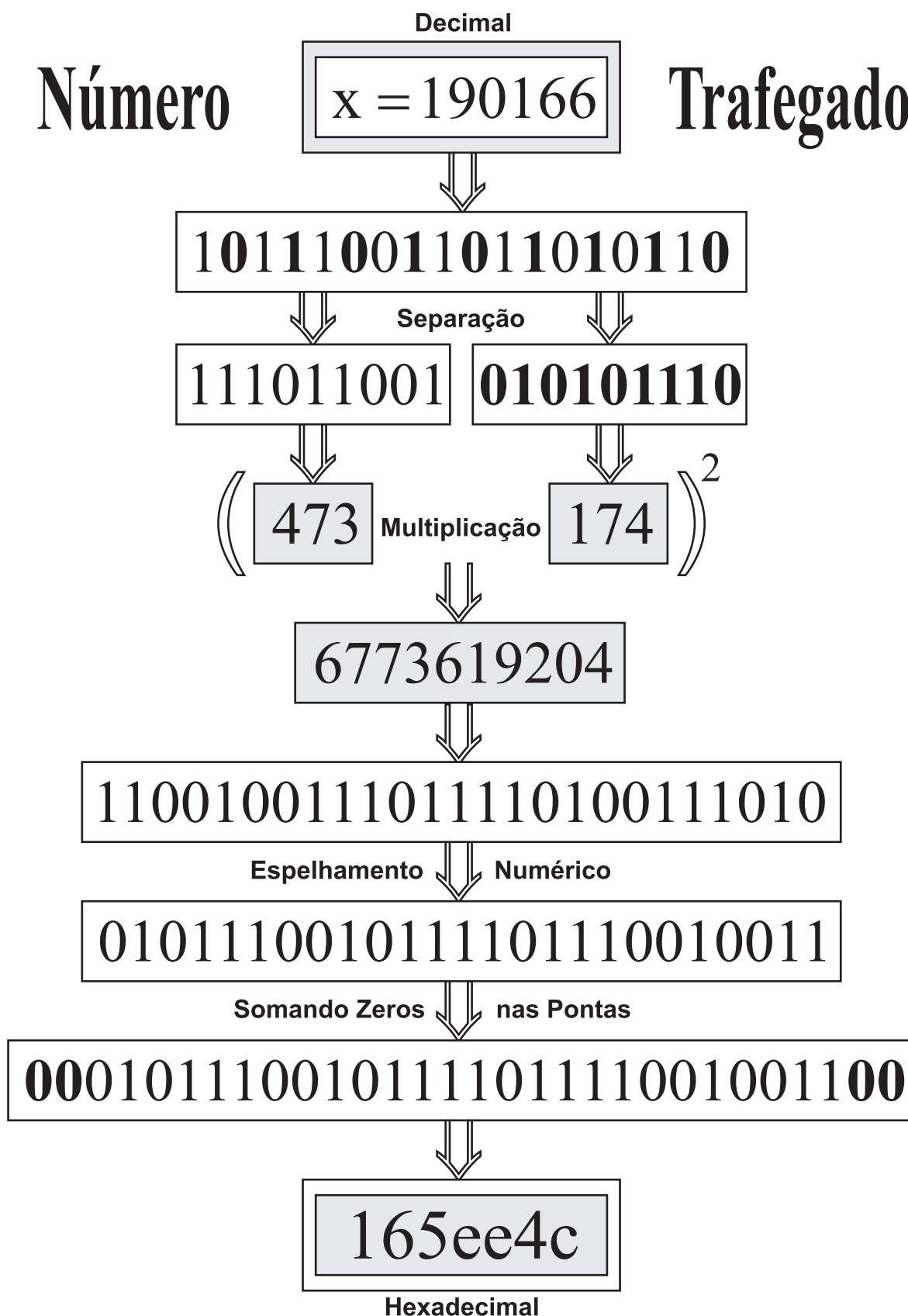
Decimal

Número Recuperado



2.3 Procedimento Computacional Unidirecional

Número **x = 190166** Trafegado



Número Irrecuperado



4.0 Hashing de Pseudorandom Numbers

$$h_{n+1}(x) = (a \cdot h_n(x) + b) \bmod m$$

$$a = 7 \quad b = 10 \quad m = 11 \quad h_0(x) = 5$$

$$\begin{aligned} *h_1(x) &= (7 \cdot h_0(x) + 10) \bmod 11 = (7 \cdot 5 + 10) \bmod 11 = 1* \\ h_2(x) &= (7 \cdot h_1(x) + 10) \bmod 11 = (7 \cdot 1 + 10) \bmod 11 = 6 \\ h_3(x) &= (7 \cdot h_2(x) + 10) \bmod 11 = (7 \cdot 6 + 10) \bmod 11 = 8 \\ h_4(x) &= (7 \cdot h_3(x) + 10) \bmod 11 = (7 \cdot 8 + 10) \bmod 11 = 0 \\ h_5(x) &= (7 \cdot h_4(x) + 10) \bmod 11 = (7 \cdot 0 + 10) \bmod 11 = 10 \\ h_6(x) &= (7 \cdot h_5(x) + 10) \bmod 11 = (7 \cdot 10 + 10) \bmod 11 = 3 \\ h_7(x) &= (7 \cdot h_6(x) + 10) \bmod 11 = (7 \cdot 3 + 10) \bmod 11 = 9 \\ h_8(x) &= (7 \cdot h_7(x) + 10) \bmod 11 = (7 \cdot 9 + 10) \bmod 11 = 7 \\ h_9(x) &= (7 \cdot h_8(x) + 10) \bmod 11 = (7 \cdot 7 + 10) \bmod 11 = 4 \\ h_{10}(x) &= (7 \cdot h_9(x) + 10) \bmod 11 = (7 \cdot 4 + 10) \bmod 11 = 5 \\ *h_{11}(x) &= (7 \cdot h_{10}(x) + 10) \bmod 11 = (7 \cdot 5 + 10) \bmod 11 = 1* \end{aligned}$$

$$\text{MDC}(a, m) = 1 \quad (m - 1) \text{ Endereços}$$

Collision Resolution k $(0, n - 1)$



5.0 Tabela ASCii e Nuances da Função Hash

	a	b	c	d	e	f	g	
ooo	97	98	99	100	101	102	103	ooo

	A	B	C	D	E	F	G	
ooo	65	66	67	68	69	70	71	ooo

Strings

1 2 3 4 5 6 7:

Ordenação

a	b	c	d	e	f	g	↔	97	98	99	100	101	102	103
---	---	---	---	---	---	---	---	----	----	----	-----	-----	-----	-----

b	c	a	e	f	g	d	↔	98	99	97	101	102	103	100
---	---	---	---	---	---	---	---	----	----	----	-----	-----	-----	-----

Letras Associadas a Números

a	b	c	d	e	f	g	↔	971	982	993	1004	1015	1026	1037
---	---	---	---	---	---	---	---	-----	-----	-----	------	------	------	------

Σ 7028

b	c	a	e	f	g	d	↔	981	992	973	1014	1025	1036	1007
---	---	---	---	---	---	---	---	-----	-----	-----	------	------	------	------

Σ 7028

Números Acrescidos a sua Ordenação para mod [2819]

$$\left(\left(1 \times 97 + 2 \times 98 + 3 \times 99 + 4 \times 100 + 5 \times 101 + 6 \times 102 + 7 \times 103 \right) \right) \text{ mod } 2819 = 9$$

$$\left(\left(1 \times 98 + 2 \times 99 + 3 \times 97 + 4 \times 101 + 5 \times 102 + 6 \times 103 + 7 \times 100 \right) \right) \text{ mod } 2819 = 0$$

$$\left(\left(1 \times 98 + 2 \times 99 + 3 \times 97 + 4 \times 101 + 5 \times 102 + 6 \times 100 + 7 \times 103 \right) \right) \text{ mod } 2819 = 3$$

(Σ Números Multiplicados pela sua Ordem) mod [2819]

(ASCii) American Standard Code For Information Interchange



23:	D	A	B	E	C	$\longleftrightarrow$	681	652	663	694	675	$\longleftrightarrow$	Σ 3365
24:	D	A	E	B	C	$\longleftrightarrow$	681	652	693	664	675	$\longleftrightarrow$	Σ 3365
25:	D	A	E	C	B	$\longleftrightarrow$	681	652	693	674	665	$\longleftrightarrow$	Σ 3365
26:	D	C	A	E	B	$\longleftrightarrow$	681	672	653	694	665	$\longleftrightarrow$	Σ 3365
27:	D	C	B	E	A	$\longleftrightarrow$	681	672	663	694	655	$\longleftrightarrow$	Σ 3365
28:	D	C	E	A	B	$\longleftrightarrow$	681	672	693	654	665	$\longleftrightarrow$	Σ 3365
29:	D	C	E	B	A	$\longleftrightarrow$	681	672	693	664	655	$\longleftrightarrow$	Σ 3365
30:	D	E	A	C	B	$\longleftrightarrow$	681	692	653	674	665	$\longleftrightarrow$	Σ 3365
31:	D	E	A	B	C	$\longleftrightarrow$	681	692	653	664	675	$\longleftrightarrow$	Σ 3365
32:	D	E	B	A	C	$\longleftrightarrow$	681	692	663	654	675	$\longleftrightarrow$	Σ 3365
33:	D	E	B	C	A	$\longleftrightarrow$	681	692	663	674	655	$\longleftrightarrow$	Σ 3365
34:	E	A	B	C	D	$\longleftrightarrow$	691	652	663	674	685	$\longleftrightarrow$	Σ 3365
35:	E	A	D	B	C	$\longleftrightarrow$	691	652	683	664	675	$\longleftrightarrow$	Σ 3365
36:	E	A	D	C	B	$\longleftrightarrow$	691	652	683	674	665	$\longleftrightarrow$	Σ 3365
37:	E	C	A	B	D	$\longleftrightarrow$	691	672	653	664	685	$\longleftrightarrow$	Σ 3365
38:	E	C	B	A	D	$\longleftrightarrow$	691	672	663	654	685	$\longleftrightarrow$	Σ 3365
39:	E	C	B	D	A	$\longleftrightarrow$	691	672	663	684	655	$\longleftrightarrow$	Σ 3365
40:	E	C	D	A	B	$\longleftrightarrow$	691	672	683	654	665	$\longleftrightarrow$	Σ 3365
41:	E	D	A	C	B	$\longleftrightarrow$	691	682	653	674	665	$\longleftrightarrow$	Σ 3365
42:	E	D	A	B	C	$\longleftrightarrow$	691	682	653	664	675	$\longleftrightarrow$	Σ 3365
43:	E	D	B	C	A	$\longleftrightarrow$	691	682	663	674	655	$\longleftrightarrow$	Σ 3365
44:	E	D	B	A	C	$\longleftrightarrow$	691	682	663	654	675	$\longleftrightarrow$	Σ 3365



7.0 Elementos Fundamentais da Construção da SHA256



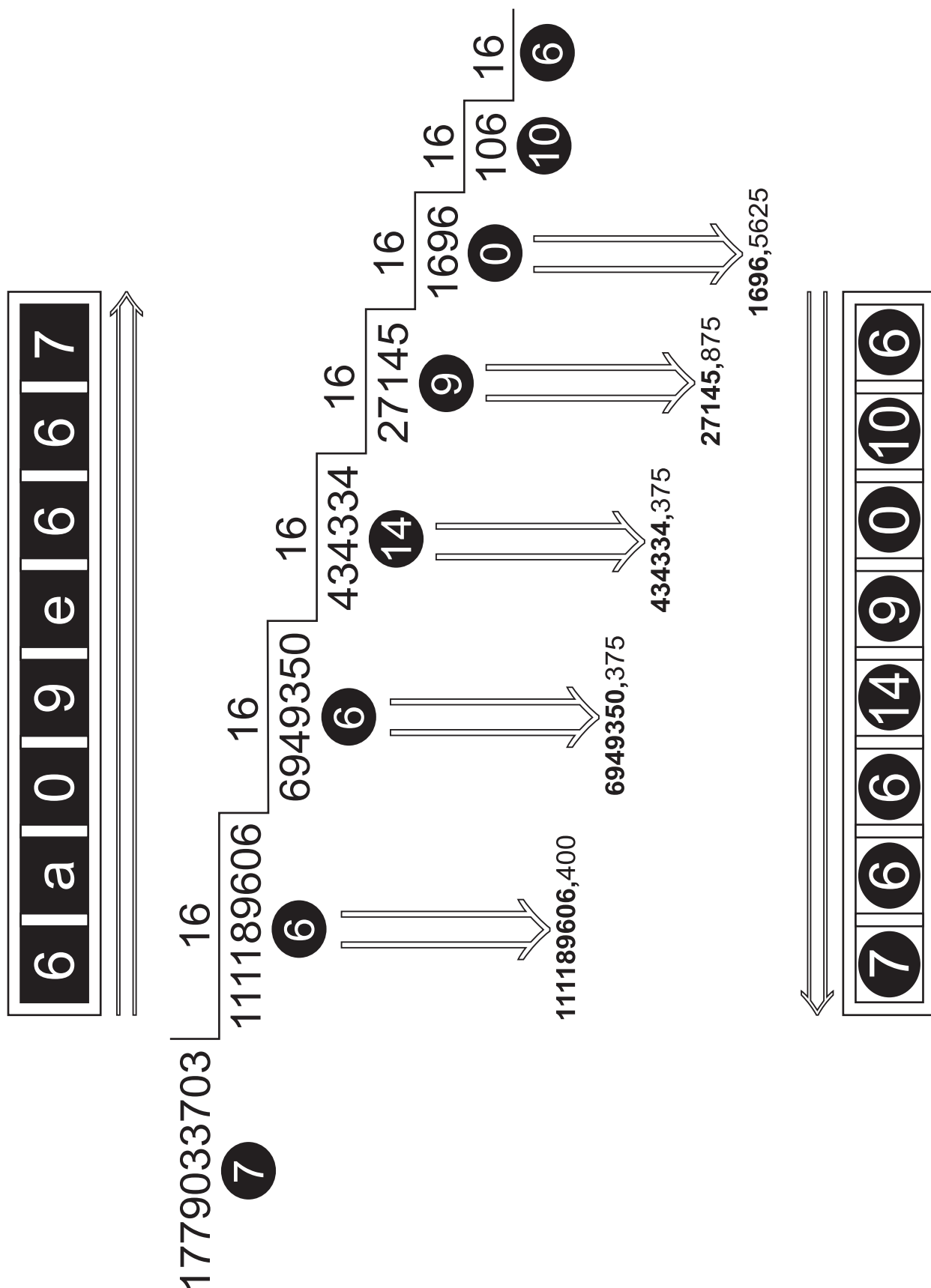
5feceb66ffc86f
38d952786c6d
696c79c2dbc23
9dd4e91b4672
9d73a27fb57e9



6b86b273ff34fc
e19d6b804eff5
a3f5747ada4ea
a22f1d49c01e5
2ddb7875b4b



14.0 Exemplo da Computação do Hexadecimal ho



(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f)



Secure Hash Algorithm

Curso de Blockchain Prandiano



Curso de Blockchaim Prandiano



n **SHA-256** **m**



d989d9aa059d7e549b05e0ff817f1641
941a6648712d2d0a78ef599e6548c14f



bf53c10ec1b5cdbe7601204935f16b71
83cccedc9da014679bf1de03cf68eba4

National Segurity Agency = NSA



	SHA256 (JASENOVSKI)	X	SHA256 (NAT. SEC. AG.)
A	559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd		559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd
B	df7e70e5021544f4834bbe64a9e3789fbc4be81470df629cad6ddb03320a5c		df7e70e5021544f4834bbe64a9e3789fbc4be81470df629cad6ddb03320a5c
C	6b23c0d5f35d1b11f9b683f0b0a617355deb11277d91ae091d399c655b87940d		6b23c0d5f35d1b11f9b683f0b0a617355deb11277d91ae091d399c655b87940d
D	3f39d5c348e5b79d06e842c114e6cc571583bbf44e4b0ebfda1a01ec05745d43		3f39d5c348e5b79d06e842c114e6cc571583bbf44e4b0ebfda1a01ec05745d43
E	a9f51566bd6705f7ea6ad54bb9deb449f795582d6529a0e22207b8981233ec58		a9f51566bd6705f7ea6ad54bb9deb449f795582d6529a0e22207b8981233ec58
F	f67ab10ad4e4c53121b6a5fe4da9c10ddee905b978d3788d2723d7bfacbe28a9		f67ab10ad4e4c53121b6a5fe4da9c10ddee905b978d3788d2723d7bfacbe28a9
G	333e0a1e27815d0ceee55c473fe3dc93d56c63bee2b3b4aee8eed6d70191a3		333e0a1e27815d0ceee55c473fe3dc93d56c63bee2b3b4aee8eed6d70191a3
H	44bd7ae60f478fae1061e11a7739f4b94d1daf917982d33b6fc8a01a63f89c21		44bd7ae60f478fae1061e11a7739f4b94d1daf917982d33b6fc8a01a63f89c21
I	a83dd0ccbffe39d071cc317ddf6e97f5c6b1c87af91919271f9fa140b0508c6c		a83dd0ccbffe39d071cc317ddf6e97f5c6b1c87af91919271f9fa140b0508c6c
J	6da43b944e494e885e69af021f93c6d9331c78aa228084711429160a5bbd15b5		6da43b944e494e885e69af021f93c6d9331c78aa228084711429160a5bbd15b5
K	86be9a55762d316a3026c2836d044f5fc76e34da10e1b45feee5f18be7edb177		86be9a55762d316a3026c2836d044f5fc76e34da10e1b45feee5f18be7edb177
L	72dfcfb0c470ac255cde83fb8fe38de8a128188e03ea5ba5b2a93adbea1062fa		72dfcfb0c470ac255cde83fb8fe38de8a128188e03ea5ba5b2a93adbea1062fa
M	08f271887ce94707da822d5263bae19d5519cb3614e0daedc4c7ce5dab7473f1		08f271887ce94707da822d5263bae19d5519cb3614e0daedc4c7ce5dab7473f1
N	8ce86a6ae65d3692e7305e2c58ac62eebd97d3d943e093f577da25c36988246b		8ce86a6ae65d3692e7305e2c58ac62eebd97d3d943e093f577da25c36988246b
O	c4694f2e93d5c4e7d51f9c5deb75e6cc8be5e1114178c6a45b6fc2c566a0aa8c		c4694f2e93d5c4e7d51f9c5deb75e6cc8be5e1114178c6a45b6fc2c566a0aa8c
P	5c62e091b8c0565f1bafad0dad5934276143ae2cce7a5381e8ada5b1a8d26d2		5c62e091b8c0565f1bafad0dad5934276143ae2cce7a5381e8ada5b1a8d26d2
Q	4ae81572f06e1b88fd5ced7a1a000945432e83e1551e6f721ee9c00b8cc33260		4ae81572f06e1b88fd5ced7a1a000945432e83e1551e6f721ee9c00b8cc33260
R	8c2574892063f995fdf756bce07f46c1a5193e54cd52837ed91e32008ccf41ac		8c2574892063f995fdf756bce07f46c1a5193e54cd52837ed91e32008ccf41ac
S	8de0b3c47f112c59745f717a626932264c422a7563954872e237b2223af4ad643		8de0b3c47f112c59745f717a626932264c422a7563954872e237b2223af4ad643
T	e632b7095b0bf32c260fa4c539e9fd7b852d0de454e9be26f24d0d6f91d069d3		e632b7095b0bf32c260fa4c539e9fd7b852d0de454e9be26f24d0d6f91d069d3
U	a25513c7e0f6eaa80a3337ee18081b9e2ed09e00af8531c8f7bb2542764027e7		a25513c7e0f6eaa80a3337ee18081b9e2ed09e00af8531c8f7bb2542764027e7
V	de5a6f78116eca62d7fc5ce159d23ae6b889b365a1739ad2cf36f925a140d0cc		de5a6f78116eca62d7fc5ce159d23ae6b889b365a1739ad2cf36f925a140d0cc
X	4b68ab3847feda7d6c62c1fbcbeebfa35eab7351ed5e78f4ddadea5df64b8015		4b68ab3847feda7d6c62c1fbcbeebfa35eab7351ed5e78f4ddadea5df64b8015
W	fc5f40df9be6bae66c1d77a6c15968866a9e6cbd7314ca432b019d17392f6f4		fc5f40df9be6bae66c1d77a6c15968866a9e6cbd7314ca432b019d17392f6f4
Y	18f5384d58bcb1bba0bcd9e6a6781d1a6ac2cc280c330ecbab6cb7931b721552		18f5384d58bcb1bba0bcd9e6a6781d1a6ac2cc280c330ecbab6cb7931b721552
Z	bbeebd879e1dff6918546dc0c179fdde505f2a21591c9a9c96e36b054ec5af83		bbeebd879e1dff6918546dc0c179fdde505f2a21591c9a9c96e36b054ec5af83

Algoritmo de Hush Espelhado

National Security Agency



	SHA256 (JASENOVSKI)	X	SHA256 (NAT. SEC. AG.)
0	5fece66ffc8f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9		5fece66ffc8f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9
1	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b		6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35		d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
3	4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce		4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce
4	4b227777d4dd1fc61c6f884f48641d02b4d121d3f32328c08b5531fcacdaf8a		4b227777d4dd1fc61c6f884f48641d02b4d121d3f32328c08b5531fcacdaf8a
5	ef2d127de37b942baad06145e54b0c619a1f22327b2ebbcfbec78f5564afe39d		ef2d127de37b942baad06145e54b0c619a1f22327b2ebbcfbec78f5564afe39d
6	e7fcc011776e8db7cd330b54174fd76f7d0216b612387a5ffcfb81e6f0919683		e7fcc011776e8db7cd330b54174fd76f7d0216b612387a5ffcfb81e6f0919683
7	7902699be42c8a8e46fbb4501726517e86b22c56a189f7625a6da49081b2451		7902699be42c8a8e46fbb4501726517e86b22c56a189f7625a6da49081b2451
8	2c624232cdd221771294dfbb310aca000a0df6ac8b66b696d90ef06defb64a3		2c624232cdd221771294dfbb310aca000a0df6ac8b66b696d90ef06defb64a3
9	19581e27de7ced00ff1ce50b2047e7a567c76b1cbaebabe5ef03f7c3017bb5b7		19581e27de7ced00ff1ce50b2047e7a567c76b1cbaebabe5ef03f7c3017bb5b7
10	4a44dc15364204a80fe80e9039455cc1608281820fe2b24f1e5233ade6af1dd5		4a44dc15364204a80fe80e9039455cc1608281820fe2b24f1e5233ade6af1dd5
11	4fc82b26aebc47d2868c4efbe3581732a3e7cbcc6c2efb32062c08170a05eeb8		4fc82b26aebc47d2868c4efbe3581732a3e7cbcc6c2efb32062c08170a05eeb8
12	6b51d431df5d7f141cbececf79edf3dd861c3b4069f0b11661a3eefacbbba918		6b51d431df5d7f141cbececf79edf3dd861c3b4069f0b11661a3eefacbbba918
13	3fdb35f04dc8c462986c992bcf875546257113072a909c162f7e470e581e278		3fdb35f04dc8c462986c992bcf875546257113072a909c162f7e470e581e278
14	8527a891e224136950ff32ca212b45bc93f69fbb801c3b1ebedac52775f99e61		8527a891e224136950ff32ca212b45bc93f69fbb801c3b1ebedac52775f99e61
15	e629fa6598d732768f7c726b4b621285f9c3b85303900aa912017db7617d8bdb		e629fa6598d732768f7c726b4b621285f9c3b85303900aa912017db7617d8bdb
16	b17ef6d19c7a5b1ee83b907c595526dcb1eb06db8227d650d5dda0a9f4ce8cd9		b17ef6d19c7a5b1ee83b907c595526dcb1eb06db8227d650d5dda0a9f4ce8cd9
17	4523540f1504cd17100c4835e85b7eefd49911580f8efff0599a8f283be6b9e3		4523540f1504cd17100c4835e85b7eefd49911580f8efff0599a8f283be6b9e3
18	4ec9599fc203d176a301536c2e091a19bc852759b255bd6818810a42c5fed14a		4ec9599fc203d176a301536c2e091a19bc852759b255bd6818810a42c5fed14a
19	9400f1b21cb527d7fa3d3eabba93557a18ebe7a2ca4e471cfe5e4c5b4ca7f767		9400f1b21cb527d7fa3d3eabba93557a18ebe7a2ca4e471cfe5e4c5b4ca7f767
20	f5ca38f748a1d6eaf726b8a42fb575c3c7f1f1864a8143301782de13da2d9202b		f5ca38f748a1d6eaf726b8a42fb575c3c7f1f1864a8143301782de13da2d9202b
21	6f4b6612125fb3a0daecd2799dfd6c9c299424fd920f9b308110a2c1fbd8f443		6f4b6612125fb3a0daecd2799dfd6c9c299424fd920f9b308110a2c1fbd8f443
22	785f3ec7eb32f30b90cd0cf3657d388b5ff4297f2f9716ff66e9b69c05ddd09		785f3ec7eb32f30b90cd0cf3657d388b5ff4297f2f9716ff66e9b69c05ddd09
23	535fa30d7e25dd8a49f1536779734ec8286108d115da5045d77f3b4185d8f790		535fa30d7e25dd8a49f1536779734ec8286108d115da5045d77f3b4185d8f790
24	c2356069e9d1e79ca924378153cfbbfb4d4416b1f99d41a2940bfd6b66c5319db		c2356069e9d1e79ca924378153cfbbfb4d4416b1f99d41a2940bfd6b66c5319db
25	b7a56873cd771f2c446d369b649430b65a756ba278ff97ec81bb6f55b2e73569		b7a56873cd771f2c446d369b649430b65a756ba278ff97ec81bb6f55b2e73569

Algoritmo de Hush Espelhado

National Security Agency