Sistemas Peer-to-Peer

3. Funções Hash Criptográficas

Francisco Sant'Anna
francisco@ime.uerj.br

Conteúdo P2P

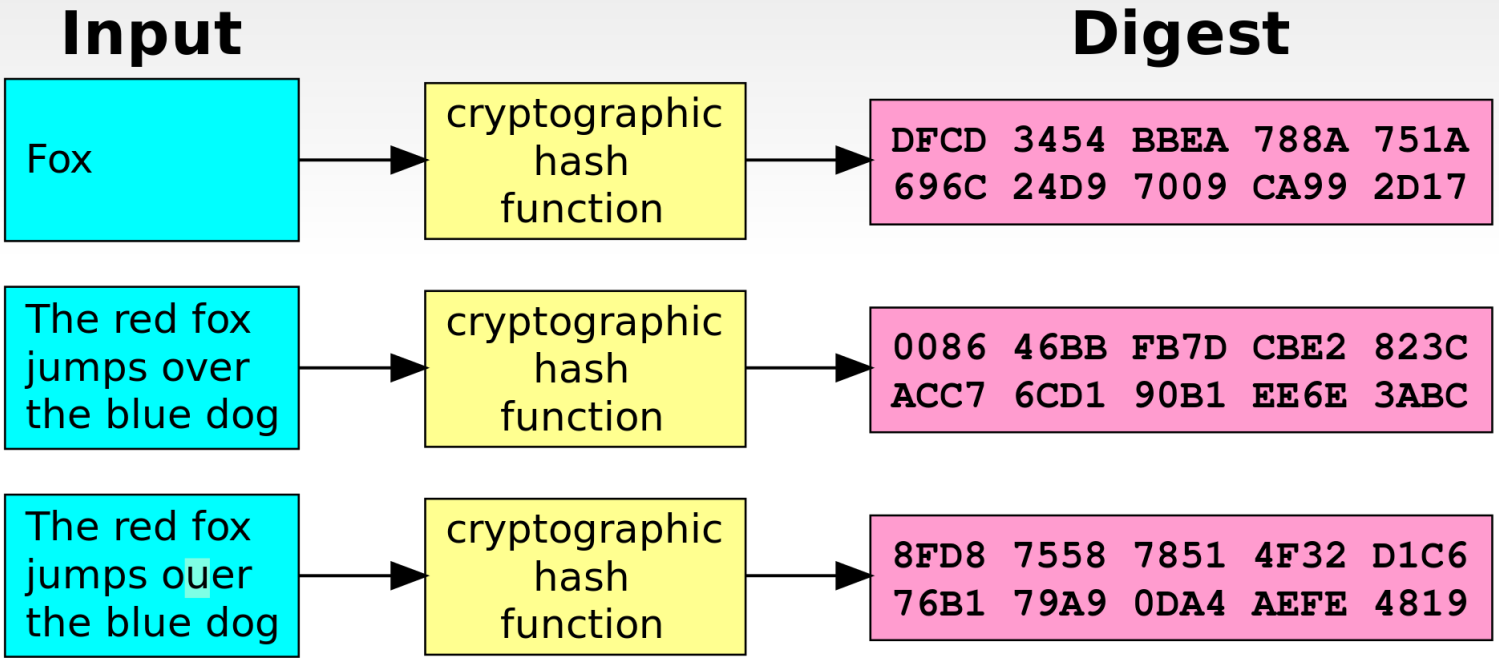
- **`GET ipfs://QmWenbjgZnA6UguLtmUYayS6e7UQM...`**
- Operações baseadas no conteúdo *(content addressing)*
- Mas...
  - … como localizar o recurso?
  - **… como identificar univocamente o recurso (dado, máquina ou pessoa)?**
  - **… como garantir integridade?**

Função Hash

- Transforma uma mensagem de tamanho arbitrário em um “resumo” de tamanho fixo:
  - `H(“muito … longa”)` → `XXXXXXXXXX`
  - `H(“abc”)` → `YYYYYYYYYY`
- Exemplo (`soma % 1000`):
  - `4D+55+49+74+6F+… = 120134` → `134`
  - `61+62+63 = 294` → `294`
  - Fácil previsibilidade

Standard 7-bit ASCII Representation							
00 nul	01 soh	02 stx	03 etx	04 eot	05 enq	06 ack	07 bel
08 bs	09 ht	0A nl	0B vt	0C np	0D cr	0E so	0F si
10 dle	11 dc1	12 dc2	13 dc3	14 dc4	15 nak	16 syn	17 etb
18 can	19 em	1A sub	1B esc	1C fs	1D gs	1E rs	1F us
20 sp	21 !	22 "	23 #	24 $	25 %	26 &	27 '
28 (	29)	2A *	2B +	2C ,	2D -	2E .	2F /
30 0	31 1	32 2	33 3	34 4	35 5	36 6	37 7
38 8	39 9	3A :	3B ;	3C <	3D =	3E >	3F ?
40 @	41 A	42 B	43 C	44 D	45 E	46 F	47 G
48 H	49 I	4A J	4B K	4C L	4D M	4E N	4F O
50 P	51 Q	52 R	53 S	54 T	55 U	56 V	57 W
58 X	59 Y	5A Z	5B [	5C \	5D]	5E ^	5F _
60 `	61 a	62 b	63 c	64 d	65 e	66 f	67 g
68 h	69 i	6A j	6B k	6C l	6D m	6E n	6F o
70 p	71 q	72 r	73 s	74 t	75 u	76 v	77 w
78 x	79 y	7A z	7B {	7C |	7D }	7E ~	7F del

Função Hash Criptográfica



Função Hash Criptográfica

- Determinística:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
- "One-way" (não inversível):
  - H^{-1}`("DFCD BBEA ... CA99 2D17") → ???`
- Sem colisões:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H(~~?????~~) → "DFCD BBEA ... CA99 2D17"`
- Caótica:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H("Foy") → "1200 C78A ... EF1A D99B"`

Aplicações

- Integridade de um recurso
  - verificar o hash após recebimento
- Identificação pequena e única de um recurso
  - o hash é a própria identificação
- Assinaturas, senhas, provas de trabalhos, etc

libsodium

Algorithm details

BLAKE2b

Notes

The `crypto_generichash_*` function set is implemented using BLAKE2b, a simple, standardized (RFC 7693) secure hash function that is as strong as SHA-3 but faster than SHA-1 and MD5.

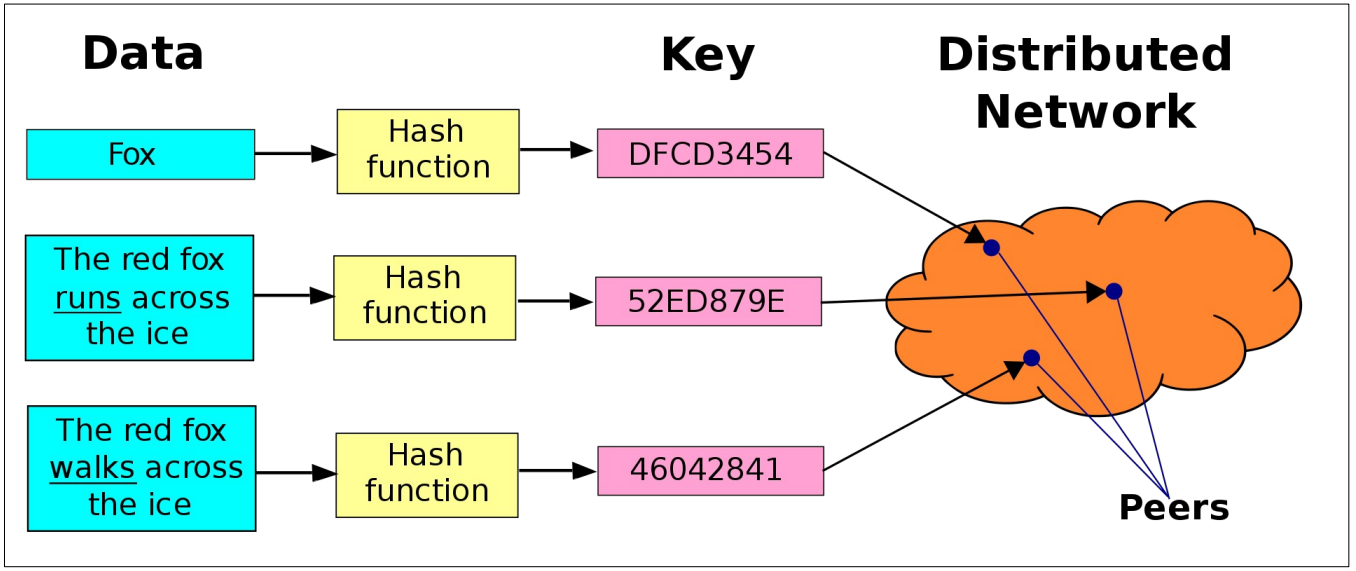
Unlike MD5, SHA-1 and SHA-256, this function is safe against hash length extension attacks.

BLAKE2b's salt and personalisation parameters are accessible through the lower-level functions whose prototypes are defined in `crypto_generichash_blake2b.h`.

BLAKE2b is not suitable for hashing passwords. For this purpose, use the `crypto_pwhash` API documented in the Password Hashing section.

Conteúdo P2P

- **`GET ipfs://QmWenbjgZnA6UguLtmUYayS6e7UQM...`**
- Operações baseadas no conteúdo *(content addressing)*
- Mas...
  - … como localizar o recurso?
  - **… como identificar univocamente o recurso (dado, máquina ou pessoa)?**
  - **… como garantir integridade?**



Exercício

- Escolha uma linguagem e uma função de hash criptográfica
  - Divulgue a sua escolha para evitar duplicatas
- Leia o conteúdo de um arquivo e exiba o seu hash
- Identifique qual é o algoritmo de hash usado pela função