CRIPTOGRAFIA NO PROC
ELEITORAL INFORMATIZ

Conceitos Básicos

Michel Kovacs
Secretário de Tecnologia da Informação
Tribunal Regional Eleitoral do Rio de Janeiro

SUM

- Hash - Resumo Criptográfico
- Assinatura Digital

H

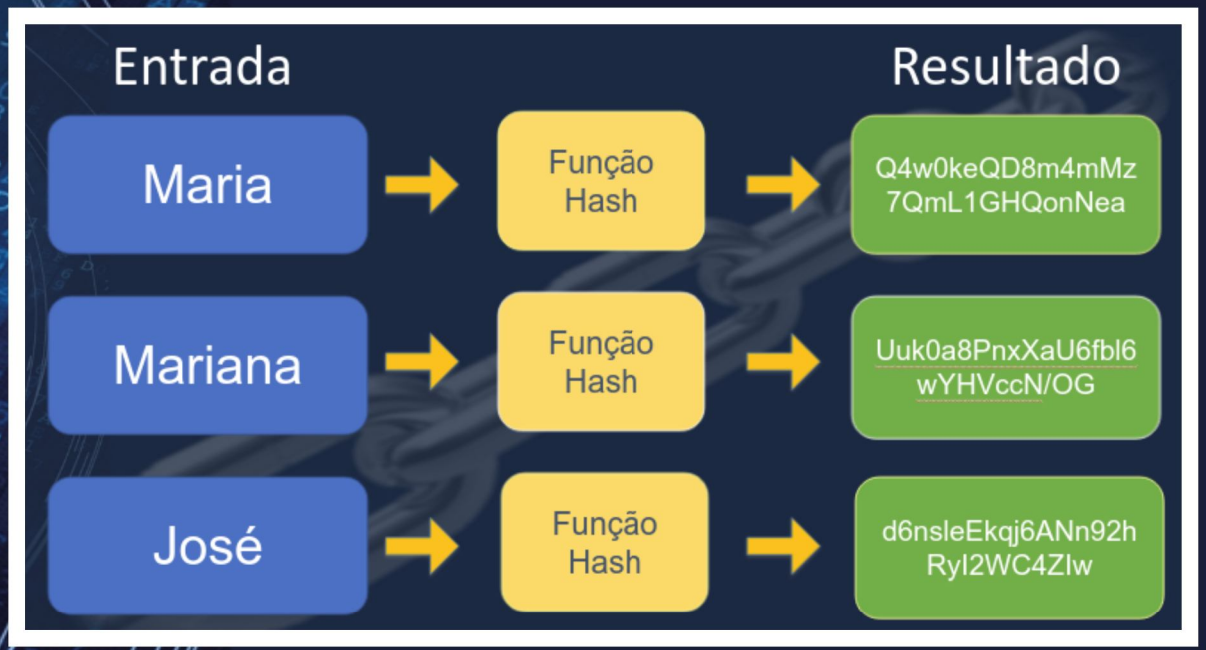
RESUMO CRIPTOGRÁ

HASH - RESUMO CRIPTOGRÁF

Como funciona?

HASH - RESUMO CRIPTOGRÁF

Quais as características? Para que serve?



- Garante a integridade de u
- Possui tamanho fixo
- Livre de “colisão”
- Algoritmos públicos
- Mesmo resultado em comp sistemas diferentes
- Garante que arquivo não f

Eleições 2020
Listagem de Hashs

Urna 2015

15/10/2020

Nome	Sha-512 Radix64
/bin/avbin.vst	Q4w0keQD8m4mMz7QmL1GHQonNea5+9lCU151S+QugFRvL3oDgVt67gdurRdZQwGf1RFsTYn
/bin/initje	Xuk0a8PnxXaU6fbl6wYHVccN/OGoeMmiie5bMWilHlSaiGMMYYpqreif+yZbiqbUBLlEnb4AhS5g
/boot/avboot.vst	+d6nsleEkqj6ANn92hRyI2WC4ZIwtlDNKGmGceYBaSQwur33xnHtqOkL/PzX0kHmiSFPeBarfy6L
/boot/uenux	9vJOD6/lgHhuwRdaWAvS/N7/eiSjJXJVDJGH3XFWmI1gdlxqxVAhP5BrFtT8RGR1Lqejo/0Bwy6g.
/etc/alsa.conf	2lzYkFFlMtj92VxnRbyGqZOWulA0/N9HrNDVhdmEjAmCezfyrYXYlXdx8JoYkyIM1ARZU4bUsl
/etc/avetc.vst	2NPg8l8sAwl+KLNQrACz7EpB8y5YIJorFWPlqbxCCEpijE22sU4k7Ctt7UcZO9N/Y3DqZe5ltdfq/pl
/etc/dependencias.properties	Yt4kn+BkBL/QVPkv7blR+ybeJj/OPc6ET+znraZuYCbOLavzp3qiSrjlJDIDhrxdZaVpz+UAuHl53sw
/etc/ld.so.cache	nTDujIeTe0s+hoJuqQrdi0mY78TPXE16ZiZwtvPwWbbd18wnMtVFSavt7wULvddIE49HwE6hEbUl
/etc/ld.so.cache.sig	7gvAMfAaheJHPz+kLP5aZXNapOEm/+Pt+QWtrob8II1FBj1MUConCzWgazlMoekz68eGzjrdvClw
/etc/ld.so.preload	GuM1JQOVguSZSaqZJk/YVyOs4U+FMwV16pbkLmwlE+1EQMkfAa52PAsJkXqBMHKRnBMKk
/etc/ld.so.preload.sig	hMQ6Vk206KeJ7jO3evWwZapBJVdmWPTaqpT+jAb4lYyOf/bdR51nI9OU/ylo/q1IptzeaslGUxGn+
/etc/versoes.properties	TRyE38M3Gzh+/flyTCxLbu8ktJmK11BNeCyUfU71XqBTNES3o7fOSigs0bwKJ7WRGoIo6HcaL2V
/etc/espeak/avespeak.vst	5kNm72rEC9x/ain1ABZLxfP5arqq9XIX3dn7JHks5RO9T+tBcsEayWazoYuKdnm8f8BSpued5DTW
/etc/espeak/intonations	KX/Gd30yNCwt30fJOZ6LzMOvZQVfxRs5vzi9O3ysHQAj1lSmMYvKqI4ipwUX/q7fVBlYfvanUnE
/etc/espeak/phondata	S8bUN5K2o/lLdtsrAyBF3qpvvia9djo8DgHxTEfo8L/hN0dtGXyYn92zTSWY8BWlJiyG/Fwjep/RHE
/etc/espeak/phonindex	nHFK+dD/iaoMkWwUROtJoyiHtzo+eZJCmBfmL+6uXEPPvsbjPPBZgX83tDhsa7sCodm7Fr7eNh3
/etc/espeak/phontab	abQ3qaTeA2J1o+TwAXxqJq6hSq5uXmHbjKKXyjvig2N6W2y+utvulRW6nZ70jrBPLHcUL7kxjNO
/etc/espeak/pt_dict	rYylOSyIDaIMAR5fQqQJ7+cmRHkBD0bOoGc3hn9gNzaby4R8mtY/Sgxj9gtOe3Vq14omUhPw8hI
/etc/espeak/lang/roa/avroa.vst	5RTXyyKwW1DklsWzvxnS3BAjR45CBq49223zb2m6Uo4tzLU0t5Lp5owECs5cAc4mrby3giBjcw2
/etc/espeak/lang/roa/pt-BR	rrV3XPYCWdNbxYF7LvmjvCowyJyCZBqQUE2agN5CbOvE4khJiauEUINegnfzEWMLadO6VfzY

ASSINATURA DIG

ASSINATURA DIGITAL

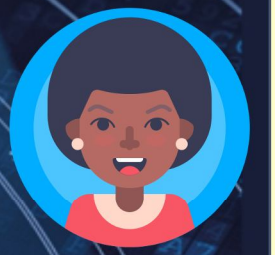
Criptografia Assimétrica

chave privada

chave p

ASSINATURA DIGITAL

Criptografia Assimétrica



Memorando 001

Ipsum lorem ipsum lorem

Atenciosamente,
Fulano

Função Hash

hash

abcd123456

criptografa
chave privada

Memorando 001

Ipsum lorem ipsum lorem

Atenciosamente,
Fulano

Função Hash

hash

abcd123456

abcd123456

ASSINATURA DIGITAL

Quais as características? Para que serve?

- Garante a **integridade** de u
- Garante a **autenticidade** de arquivo
- Garante a **autoria** de um ar
- Algoritmos públicos
- **Mesmo resultado** em comp sistemas diferentes

OBRIGADO!