Autenticação Digital

Grupo de Resposta a Incidentes de Segurança

OLÁ,

Eu sou João Pedro Wieland

Aluno de Engenharia Eletrônica e de Computação na UFRJ, Diretor do GRIS e membro da Equipe SIGA.

Eu sou Sidney Outeiro

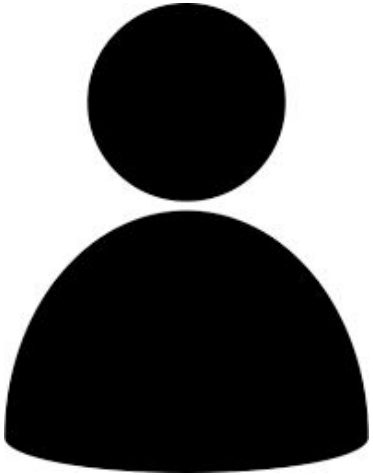
Aluno de Ciência da Computação, membro do GRIS e membro do Labnet

É o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira. ”

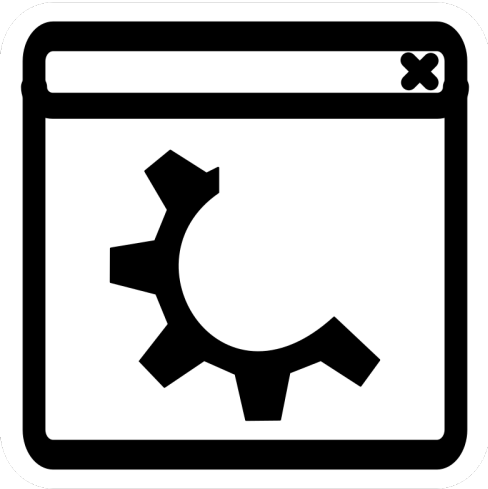
No mundo analógico...

Uma pessoa da fé ao documento

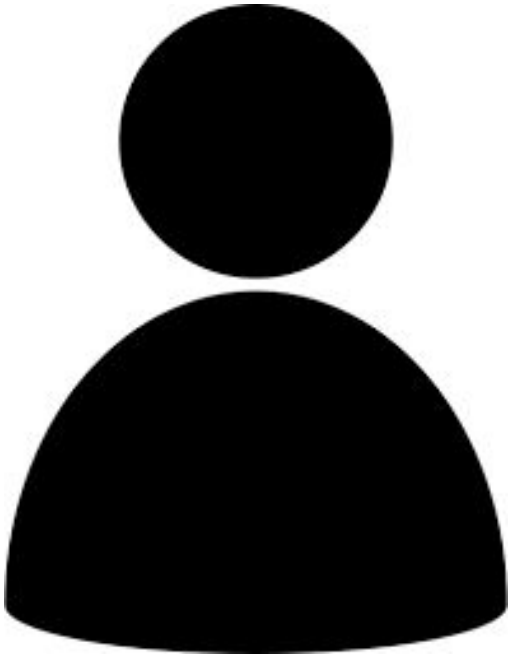
O que deve ser autenticado?

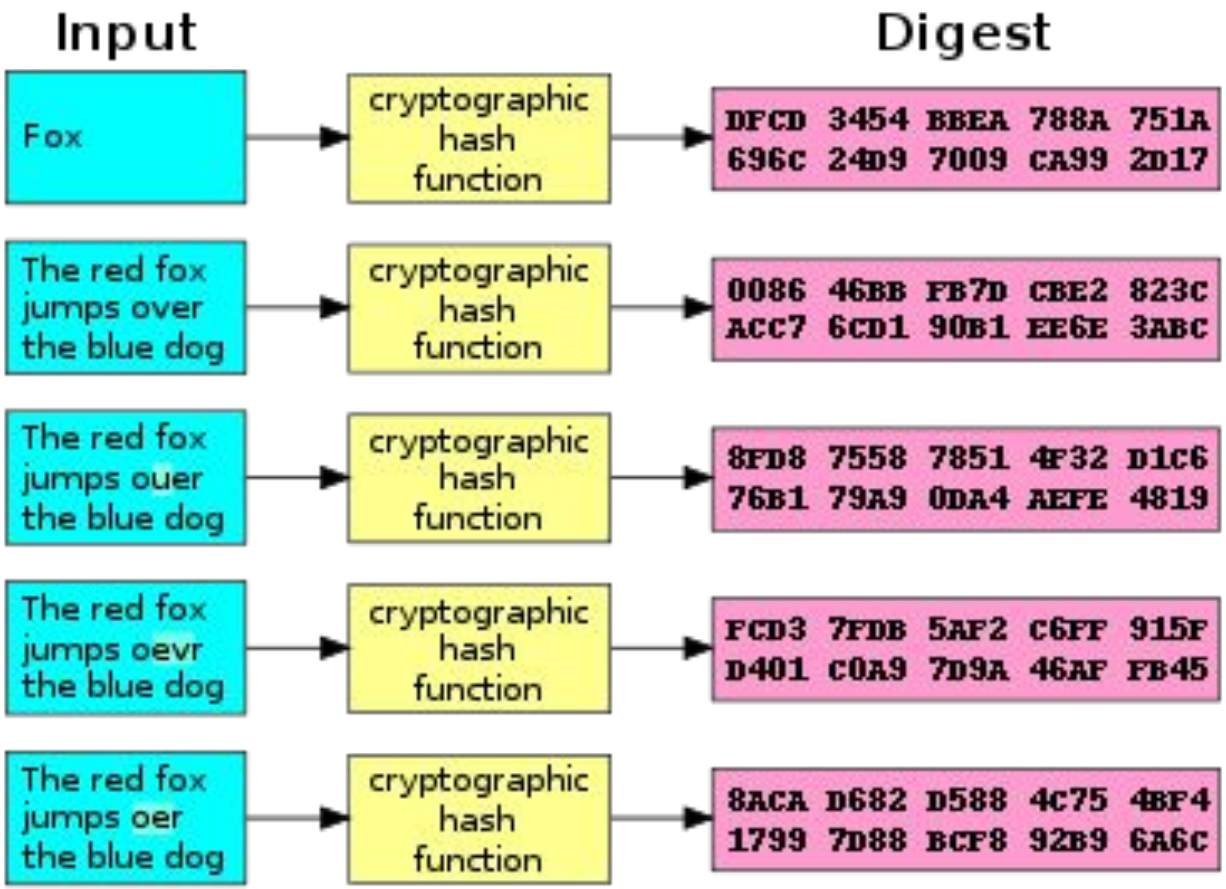


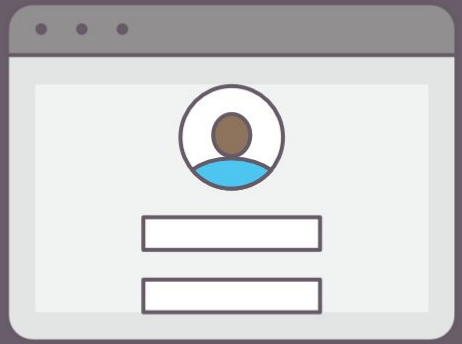
Usuários



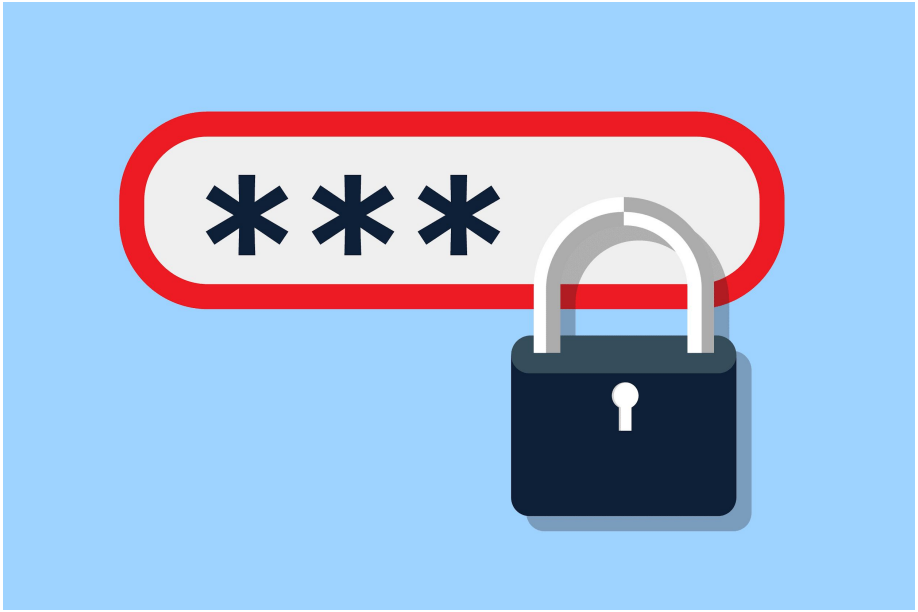
Aplicações



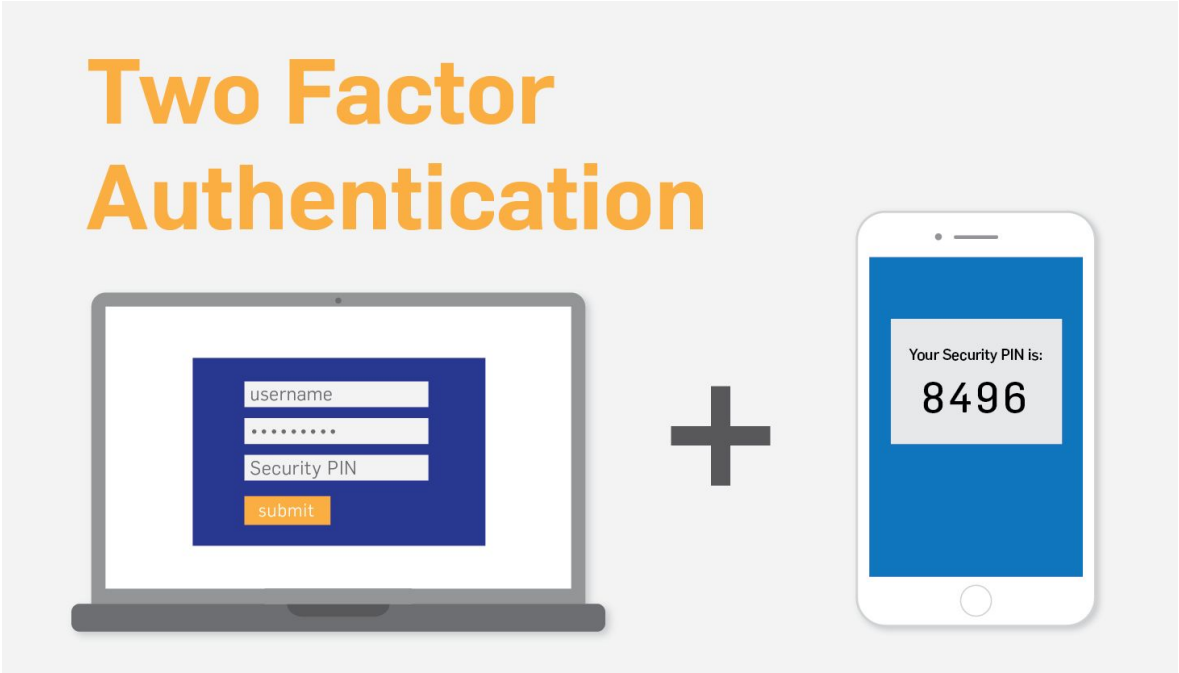

Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C



Senha



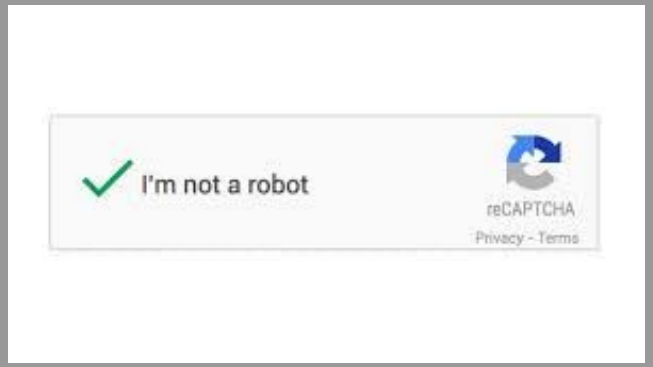
Autenticação de duas etapas

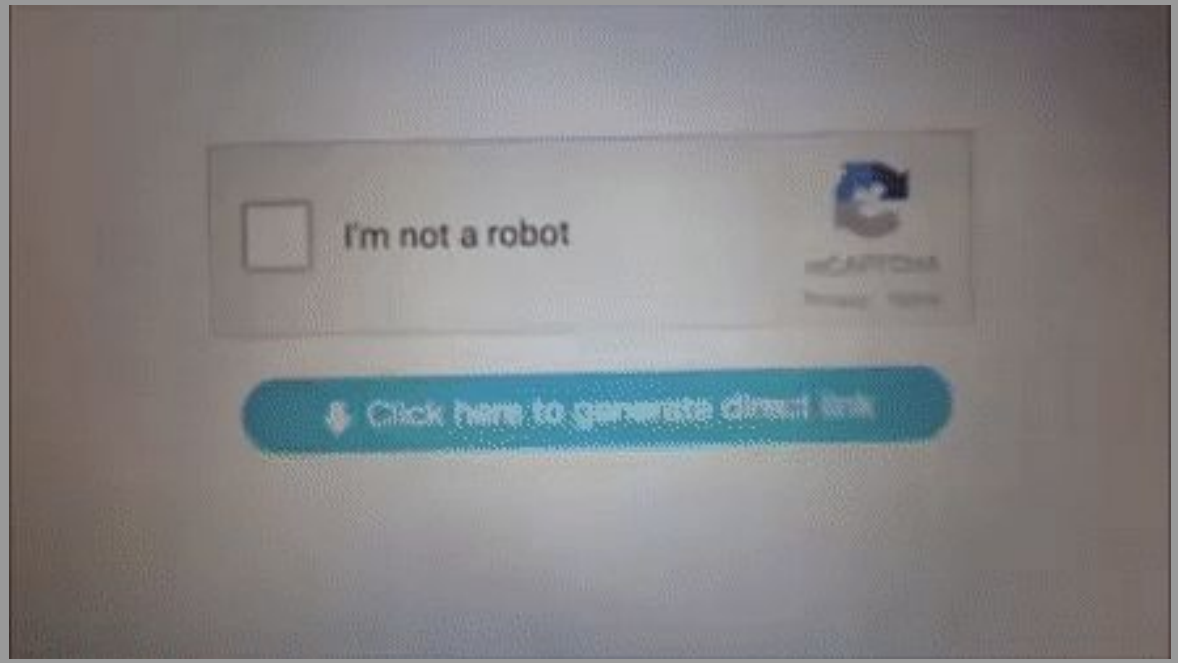


CAPTCHA

- **Os CAPTCHAs foram desenvolvidos em 1997 como uma resposta à ataques de bots usando OCR (*Optical Character Recognition*)**
- **Os primeiros CAPTCHAs foram usados no site AltaVista**

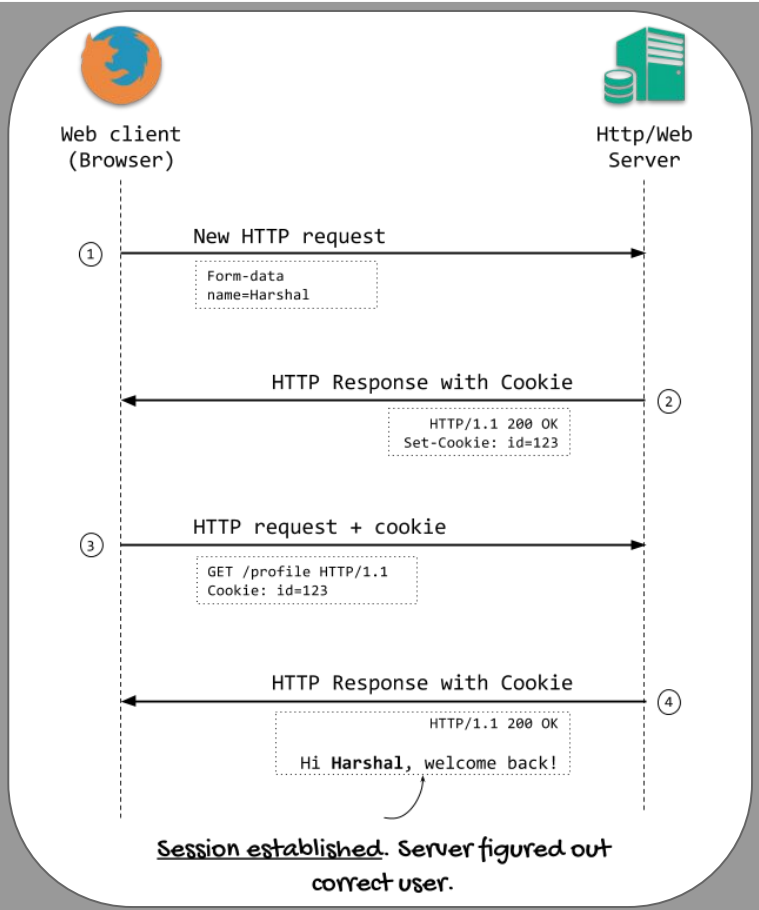

overlooks
inquiry
Type the two words:
reCAPTCHA™
stop spam.
read books.


I'm not a robot
reCAPTCHA
Privacy - Terms


I'm not a robot
reCAPTCHA
Click here to generate direct link

Cookie

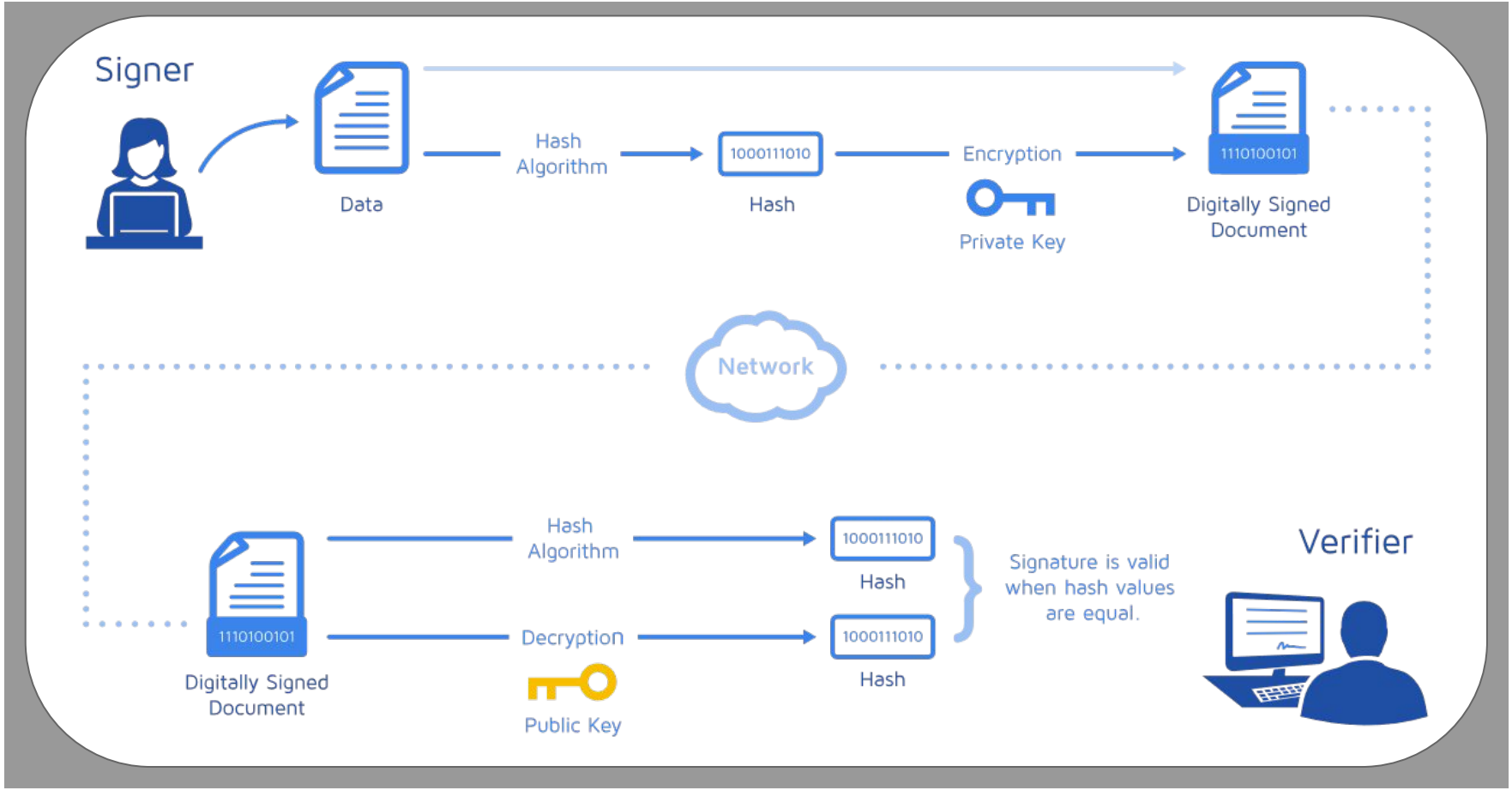
- **Um cookie é um pacote de dados enviados de um site ao navegador, para que a cada vez que o usuário acesse novamente o site o cookie é enviado contendo as atividades prévias do usuário.**

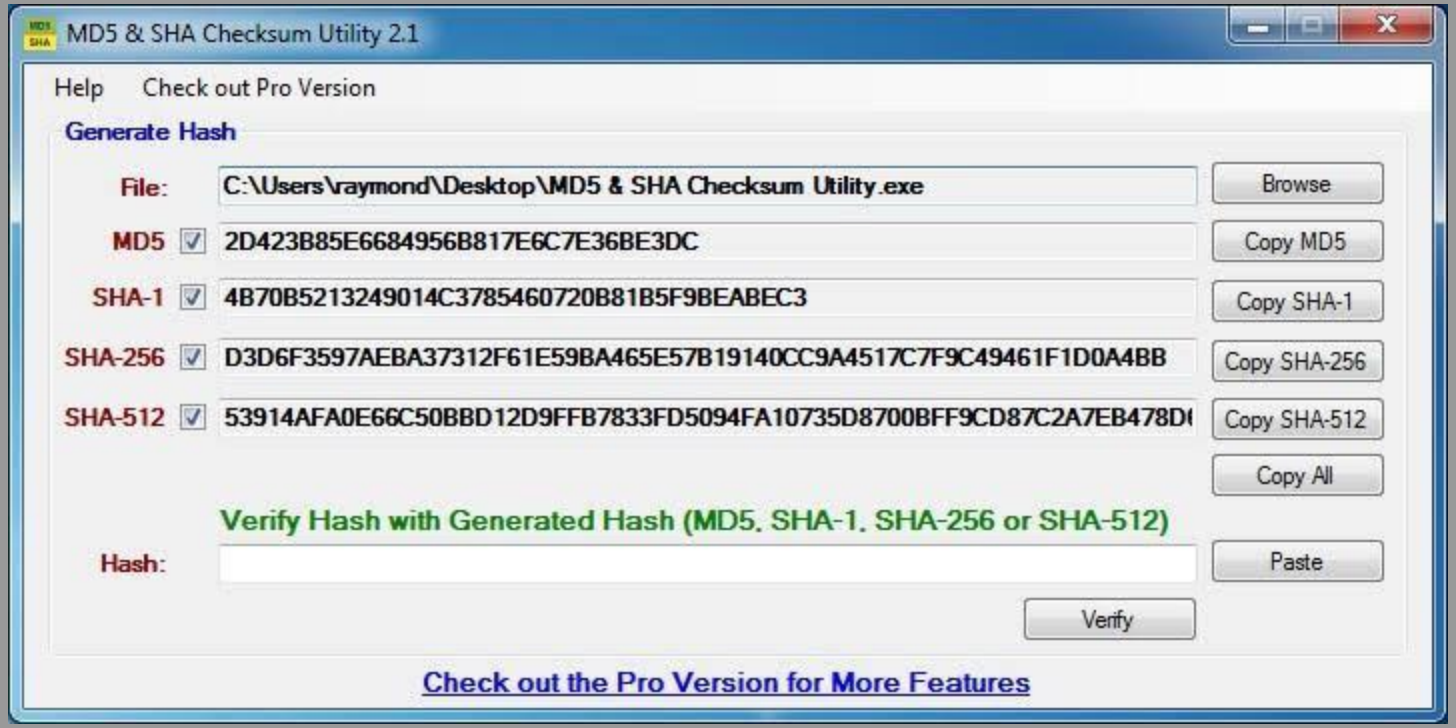

Web client
(Browser)
Http/Web
Server
1
New HTTP request
Form-data
name=Harshal
HTTP Response with Cookie
2
HTTP/1.1 200 OK
Set-Cookie: id=123
3
HTTP request + cookie
GET /profile HTTP/1.1
Cookie: id=123
HTTP Response with Cookie
4
HTTP/1.1 200 OK
Hi Harshal, welcome back!
Session established. Server figured out
correct user.

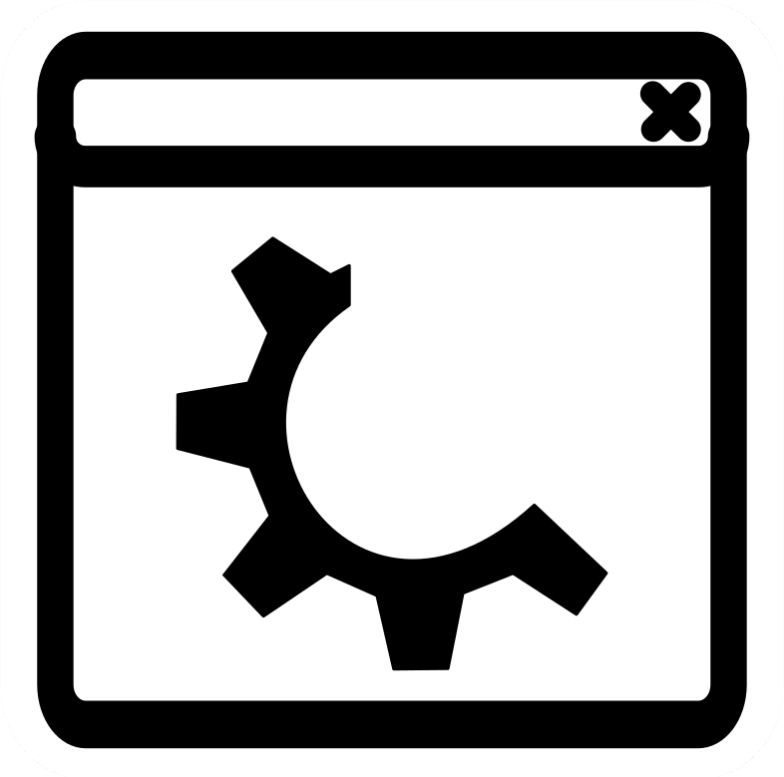
Domain	Path	Content	Expires	Secure
gris-casino.com	**/**	**UserID=87342**	**31/02/2077**	**Yes**
gris-loja.com	**/**	**Cart=7-392;3-578**	**19/01/1893**	**No**

Assinatura Digital

- **A partir de uma função hash e um sistema de chave pública podemos garantir a autenticidade, integridade e irretratabilidade de uma mensagem ou documento**

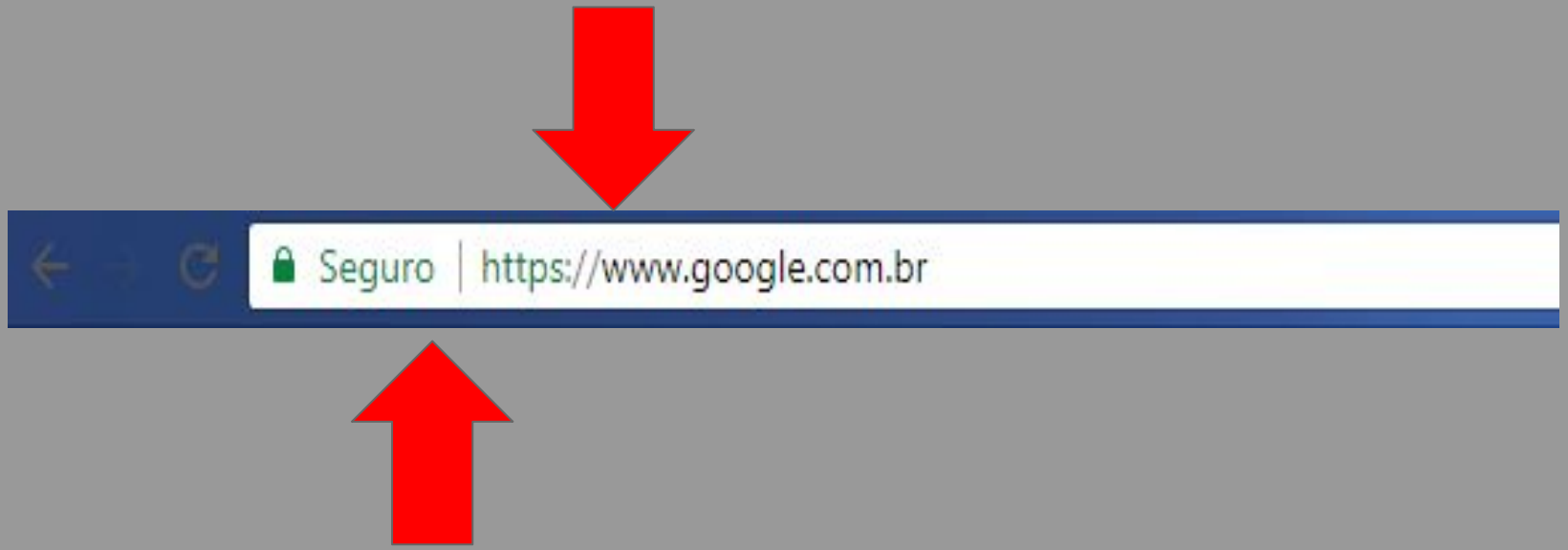

Signer
Data
Hash Algorithm
1000111010
Hash
Encryption
Private Key
1110100101
Digitally Signed Document
Network
1110100101
Digitally Signed Document
Hash Algorithm
1000111010
Hash
Decryption
Public Key
1000111010
Hash
Signature is valid when hash values are equal.
Verifier


MD5 & SHA Checksum Utility 2.1
Help
Check out Pro Version
Generate Hash
File:
C:\Users\raymond\Desktop\MD5 & SHA Checksum Utility.exe
Browse
MD5
2D423B85E6684956B817E6C7E36BE3DC
Copy MD5
SHA-1
4B70B5213249014C3785460720B81B5F9BEABEC3
Copy SHA-1
SHA-256
D3D6F3597AEBA37312F61E59BA465E57B19140CC9A4517C7F9C49461F1D0A4BB
Copy SHA-256
SHA-512
53914AFA0E66C50BBD12D9FFB7833FD5094FA10735D8700BFF9CD87C2A7EB478D
Copy SHA-512
Copy All
Verify Hash with Generated Hash (MD5, SHA-1, SHA-256 or SHA-512)
Hash:
Paste
Verify
Check out the Pro Version for More Features



Certificado SSL

- **Com o objetivo de proteger dados sensíveis, o certificado SSL garante um nível de confiança a um domínio web através do uso da criptografia durante a comunicação servidor-cliente**


Seguro
https://www.google.com.br

OBRIGADO


jpvbwieland@poli.ufrj.br


@joaowieland


sid@dcc.ufrj.br


@outeirosid