A survey into CDNs Security

Costa, Lucas B.[1] Maziero, Carlos A.[2]

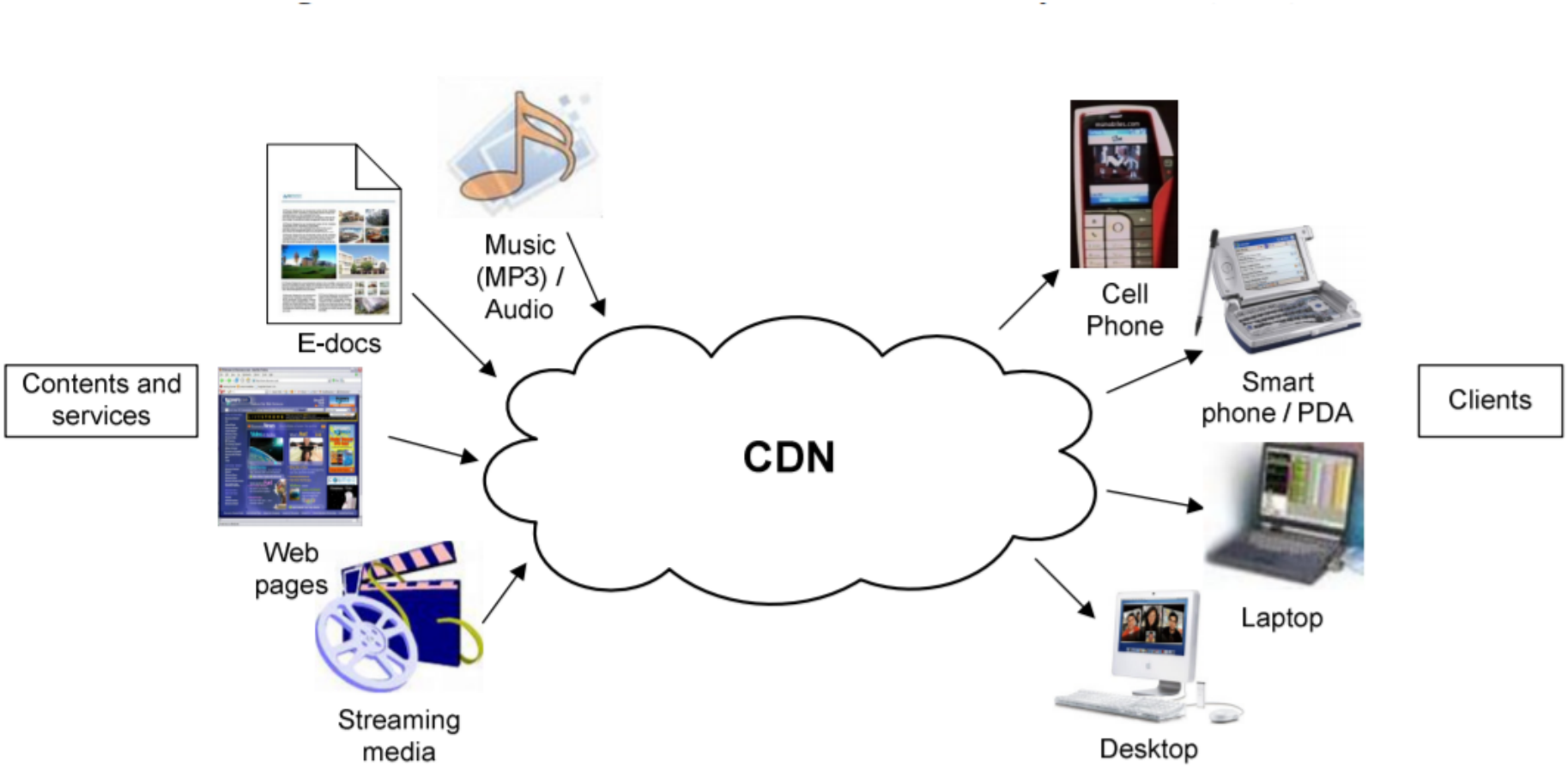
[1]Departamento de Informática
UFPR

Dezembro, 2018

Sumário

Sumário

Contextualização



Sumário

Composição de uma CDN

- Organização.

Composição de uma CDN

- Organização.
- Tipos de servidores.

Composição de uma CDN

- Organização.
- Tipos de servidores.
- Tipos de relacionamentos.

Composição de uma CDN

- Organização.
- Tipos de servidores.
- Tipos de relacionamentos.
- Protocolos de interações.

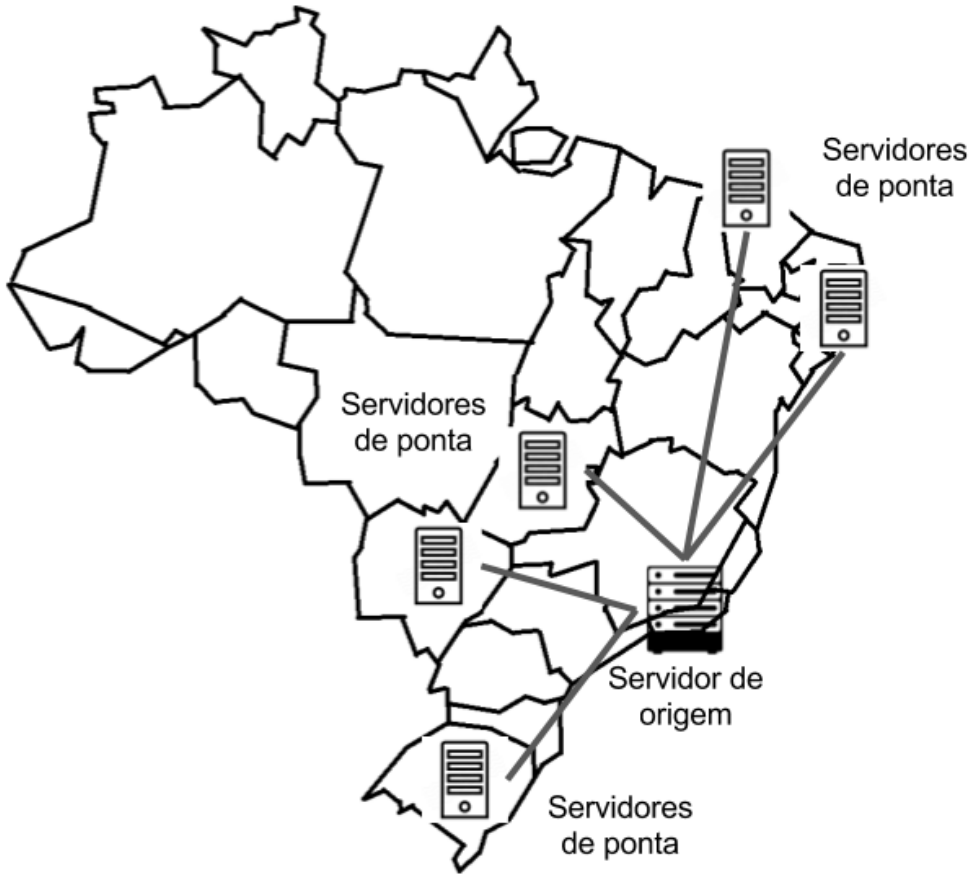
Composição de uma CDN

- Organização.
- Tipos de servidores.
- Tipos de relacionamentos.
- Protocolos de interações.
- Tipos de conteúdos.

Sumário

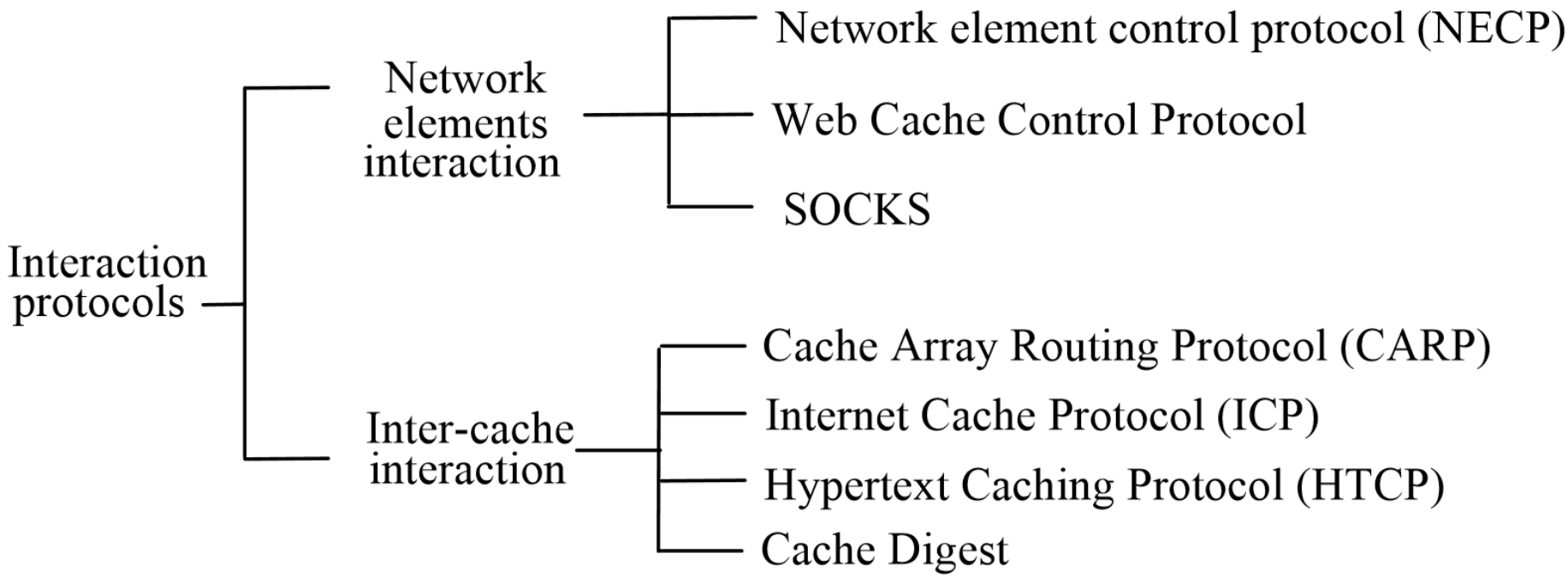
Tipos de servidores

- Servidor de origem
- Servidor de ponta



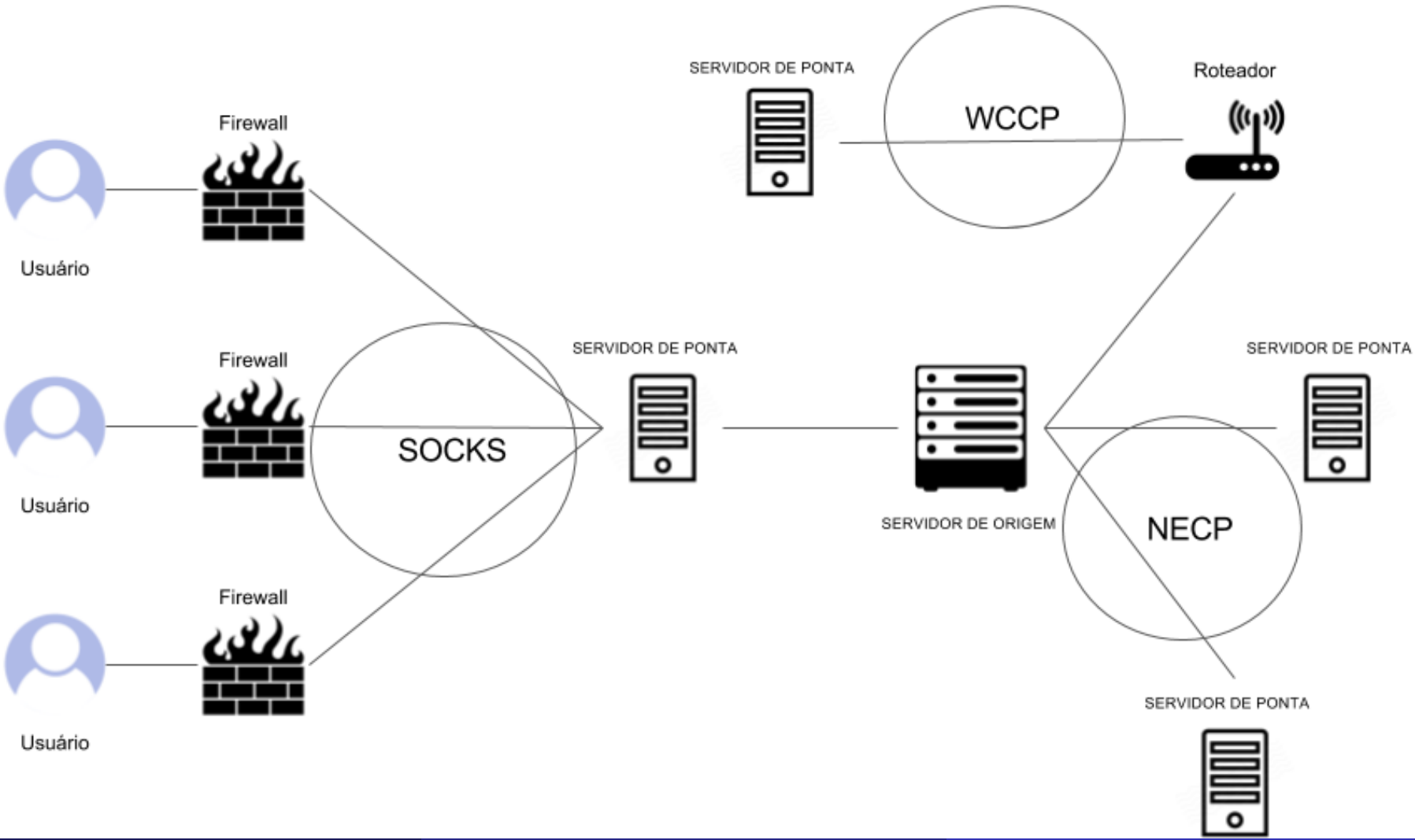
Sumário

Protocolos de interações



Protocolos de interações

Interações dos elementos da rede



HTCP - Hypertext Caching Protocol

- Protocolo para descobri Caches HTTP;
- Suporte ao HTTP 1.0;
- Permite incluir cabealhos nas respostas;
- Podem ser enviados via TCP/UDP;
- Devem ser resilientes à falhas.

ICP - Internet Cache Protocol

- Protocolo de mensagem leve;
- Utilizado para comunicação de Caches;
- Utiliza consultas para determinar localização mais apropriada;
- Suporte ao HTTP 0.9;
- Comunica-se com caches vizinhos;
- recebe MISS ou HIT como resposta;
- Enviado via UDP;
- Falha por timeout indica caminho quebrado;
- Fornece informações para balanceamento através das medidas de perda.

HTCP x ICP

- HTCP permite envio via UDP e TCP;
- HTCP permite incluir apenas os cabealhos nas respostas;
- HTCP consegue monitorar conteúdo de caches remotos(não vizinhos)
- ICP permite monitoramento de falhas e assim controle para balanceamento

Protocolos de interações

Interações de cache

CARP - Cache Array Routing Protocol Protocolo de armazenamento distribuído baseado em uma lista conhecida de proxies suavemente acoplada e uma função hash para dividir o espaço URL entre esses proxies.

- Cliente HTTP pode enviar requisição à qualquer proxy da lista.

Protocolos de interações

Interações de cache

Cache Digest Protocolo de intercâmbio e formato de dados entre caches.

- Fornecem um resumo dos conteúdos na resposta;
- Soluciona os problemas de congestionamento e timeout;
- Torna possível determinar se um servidor possui em cache um conteúdo;
- Executado via HTTP ou FTP;
- Contém tempo de expiração na resposta;
- Podem ser utilizados para eliminar redundância.

Sumário

Tipos de seleção

- Full - site
- Partial - site

Tipos de modos de seleção

Full - site

- Entrega total de conteúdo.

Tipos de modos de seleção

Partial - site

Tipos de distribuição:

- Empirico
- Popularidade

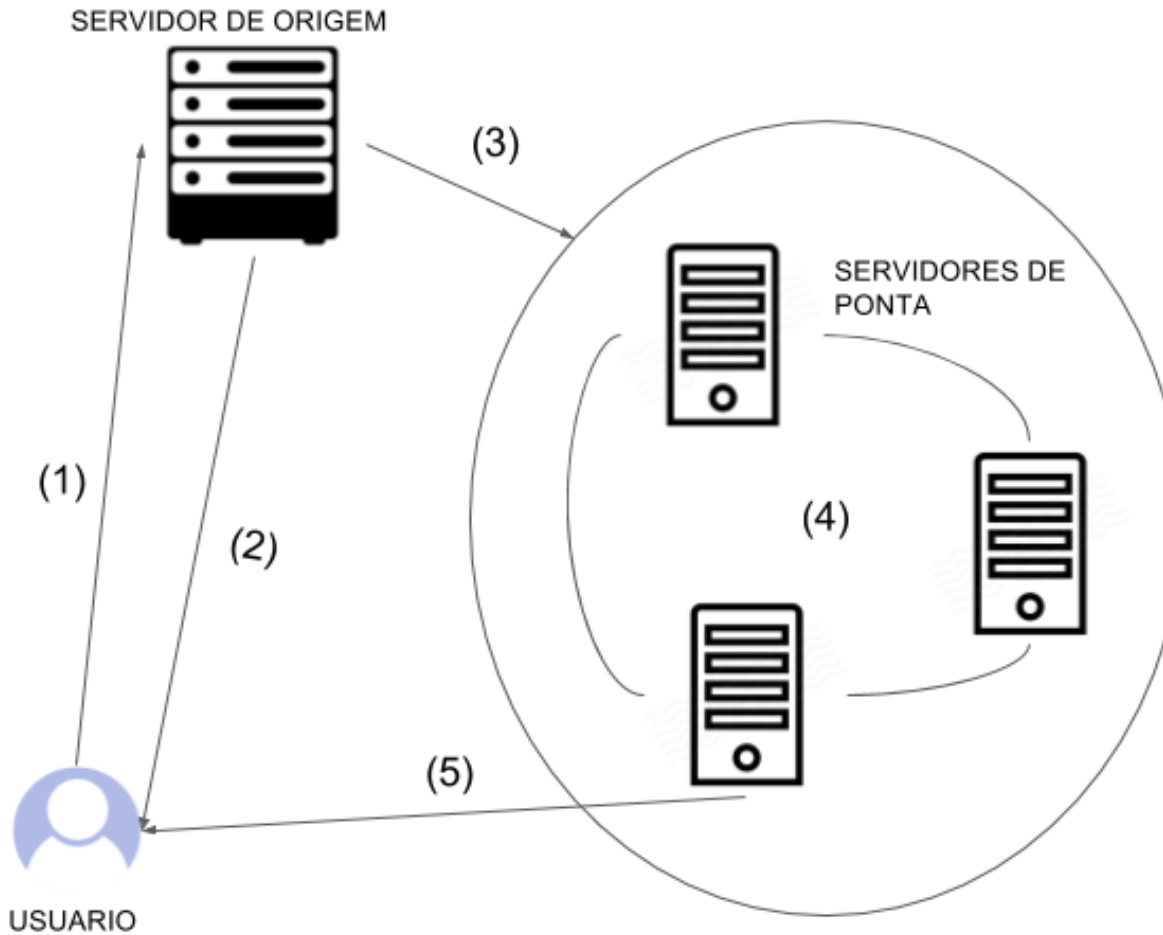
Tipos de aglomerações:

- Objeto
- Conjunto de objetos

Entrega de conteúdo

Partial-site

(1)	Requista rota
(2)	Retorna um index.html
(3)	redireciona a requisição para o provedor de CDN
(4)	Acha o melhor servidor de ponta
(5)	Envia o conteúdo ao usuário



VOD - Video On Demand

Envio da URL para o player

http

No.	Time	Source	Destination	Protocol	Length	Info
12278	2.081222	192.168.15.8	192.168.15.7	HTTP	288	PUT /player/18cd39/stop HTTP/1.1
12328	2.084946	192.168.15.8	192.168.15.7	HTTP	339	PUT /player/18cd39/play HTTP/1.1 (application/json)
29501	4.105385	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
29521	4.107044	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
29815	4.131296	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
30697	4.201873	201.0.52.15	192.168.15.7	HTTP	635	HTTP/1.1 200 OK (application/manifest)
31441	4.287982	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
31456	4.289669	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
31590	4.300898	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
36377	4.844038	201.0.52.15	192.168.15.7	MP4	724	
36782	4.869234	201.0.52.15	192.168.15.7	MP4	1542	
37006	4.954702	192.168.15.7	201.0.52.15	HTTP	322	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=2

```
> Frame 12328: 339 bytes on wire (2712 bits), 339 bytes captured (2712 bits)
> Ethernet II, Src: Digibras_87:db:dd (64:1c:67:87:db:dd), Dst: ArrisGro_b8:39:dc (20:f1:9e:b8:39:dc)
> Internet Protocol Version 4, Src: 192.168.15.8, Dst: 192.168.15.7
> Transmission Control Protocol, Src Port: 42096, Dst Port: 80, Seq: 225, Ack: 1, Len: 273
> [2 Reassembled TCP Segments (497 bytes): #12294(224), #12328(273)]
> Hypertext Transfer Protocol
v JavaScript Object Notation: application/json
  v Object
    v Member Key: play_info
        String value: http://o2.b38489.cdn.telefonica.com/38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest|ifmt=mss
        Key: play_info
    > Member Key: timeshift_enabled
    > Member Key: metadata
```

VOD - Video On Demand

Get da URL para CDN

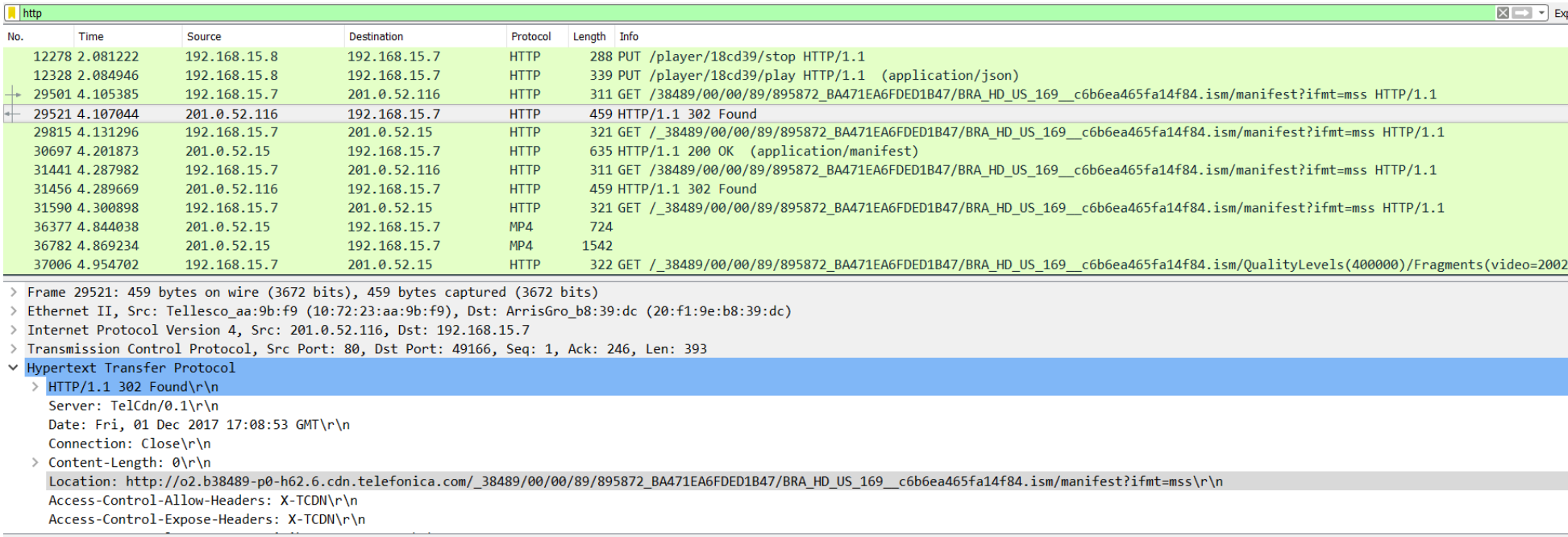
http

No.	Time	Source	Destination	Protocol	Length	Info
12278	2.081222	192.168.15.8	192.168.15.7	HTTP	288	PUT /player/18cd39/stop HTTP/1.1
12328	2.084946	192.168.15.8	192.168.15.7	HTTP	339	PUT /player/18cd39/play HTTP/1.1 (application/json)
29501	4.105385	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
29521	4.107044	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
29815	4.131296	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
30697	4.201873	201.0.52.15	192.168.15.7	HTTP	635	HTTP/1.1 200 OK (application/manifest)
31441	4.287982	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
31456	4.289669	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
31590	4.300898	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
36377	4.844038	201.0.52.15	192.168.15.7	MP4	724	
36782	4.869234	201.0.52.15	192.168.15.7	MP4	1542	
37006	4.954702	192.168.15.7	201.0.52.15	HTTP	322	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=200

```
> Frame 29501: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)
> Ethernet II, Src: ArrisGro_b8:39:dc (20:f1:9e:b8:39:dc), Dst: Tellesco_aa:9b:f9 (10:72:23:aa:9b:f9)
> Internet Protocol Version 4, Src: 192.168.15.7, Dst: 201.0.52.116
> Transmission Control Protocol, Src Port: 49166, Dst Port: 80, Seq: 1, Ack: 1, Len: 245
v Hypertext Transfer Protocol
  > GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1\r\n
    Host: o2.b38489.cdn.telefonica.com\r\n
    User-Agent: libcurl/7.43.0 OpenSSL/1.0.1t zlib/1.2.8\r\n
    Accept: */*\r\n
    Accept-Encoding: deflate, gzip\r\n
    \r\n
    [Full request URI: http://o2.b38489.cdn.telefonica.com/38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss]
    [HTTP request 1/1]
```

VOD - Video On Demand

Retorno da URL no campo location



http

No.	Time	Source	Destination	Protocol	Length	Info
12278	2.081222	192.168.15.8	192.168.15.7	HTTP	288	PUT /player/18cd39/stop HTTP/1.1
12328	2.084946	192.168.15.8	192.168.15.7	HTTP	339	PUT /player/18cd39/play HTTP/1.1 (application/json)
29501	4.105385	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
29521	4.107044	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
29815	4.131296	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
30697	4.201873	201.0.52.15	192.168.15.7	HTTP	635	HTTP/1.1 200 OK (application/manifest)
31441	4.287982	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
31456	4.289669	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
31590	4.300898	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
36377	4.844038	201.0.52.15	192.168.15.7	MP4	724	
36782	4.869234	201.0.52.15	192.168.15.7	MP4	1542	
37006	4.954702	192.168.15.7	201.0.52.15	HTTP	322	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=2002

```
> Frame 29521: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits)
> Ethernet II, Src: Tellesco_aa:9b:f9 (10:72:23:aa:9b:f9), Dst: ArrisGro_b8:39:dc (20:f1:9e:b8:39:dc)
> Internet Protocol Version 4, Src: 201.0.52.116, Dst: 192.168.15.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 49166, Seq: 1, Ack: 246, Len: 393
v Hypertext Transfer Protocol
  > HTTP/1.1 302 Found\r\n
    Server: TelCdn/0.1\r\n
    Date: Fri, 01 Dec 2017 17:08:53 GMT\r\n
    Connection: Close\r\n
  > Content-Length: 0\r\n
    Location: http://o2.b38489-p0-h62.6.cdn.telefonica.com/_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss\r\n
    Access-Control-Allow-Headers: X-TCDN\r\n
    Access-Control-Expose-Headers: X-TCDN\r\n
```

VOD - Video On Demand

Download do chunck direto da URL

http

No.	Time	Source	Destination	Protocol	Length	Info
29501	4.105385	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
29521	4.107044	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
29815	4.131296	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
30697	4.201873	201.0.52.15	192.168.15.7	HTTP	635	HTTP/1.1 200 OK (application/manifest)
31441	4.287982	192.168.15.7	201.0.52.116	HTTP	311	GET /38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
31456	4.289669	201.0.52.116	192.168.15.7	HTTP	459	HTTP/1.1 302 Found
31590	4.300898	192.168.15.7	201.0.52.15	HTTP	321	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/manifest?ifmt=mss HTTP/1.1
36377	4.844038	201.0.52.15	192.168.15.7	MP4	724	
36782	4.869234	201.0.52.15	192.168.15.7	MP4	1542	
37006	4.954702	192.168.15.7	201.0.52.15	HTTP	322	GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=20
40391	5.304082	192.168.15.7	201.0.52.15	HTTP	325	[TCP ACKed unseen segment] [TCP Previous segment not captured] GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169
48581	6.256095	201.0.52.15	192.168.15.7	HTTP	1506	[TCP ACKed unseen segment] [TCP Previous segment not captured] Continuation

```
> Frame 37006: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits)
> Ethernet II, Src: ArrisGro_b8:39:dc (20:f1:9e:b8:39:dc), Dst: Tellesco_aa:9b:f9 (10:72:23:aa:9b:f9)
> Internet Protocol Version 4, Src: 192.168.15.7, Dst: 201.0.52.15
> Transmission Control Protocol, Src Port: 40969, Dst Port: 80, Seq: 193, Ack: 84000, Len: 256
v Hypertext Transfer Protocol
  > GET /_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=20020000) HTTP/1.1\r\n
    Host: o2.b38489-p0-h62.6.cdn.telefonica.com\r\n
    User-Agent: Mozilla/5.0-OpenSTB-2017.11.27.00.01.59-MSS\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://o2.b38489-p0-h62.6.cdn.telefonica.com/_38489/00/00/89/895872_BA471EA6FDED1B47/BRA_HD_US_169__c6b6ea465fa14f84.ism/QualityLevels(400000)/Fragments(video=20020000)]
    [HTTP request 2/5]
    [Next request in frame: 52827]
```

Sumário

Caching

Tipos

- Intra-cluster
  - Por pesquisa;
  - Por síntese;
  - Por diretório;
  - Por hashing;
  - Por semi-hashing.
- Inter-cluster
  - Por pesquisa.

Caching

Intra-cluster

- Por pesquisa:
  - Uma pesquisa(consulta) é enviada de um cache para outro;
  - Latência é um problema;
  - Alto tráfego de informação;
  - Espera receber "HIT"ou "MISS".
- Por síntese:
  - Cada servidor mantém um resumo dos conteúdos dos outros;
  - Todos os caches subescritos são informados sobre mudanças;
  - Alto tráfego em casos de muitas atualizações;
- Por diretório:
  - Versão centralizada do por síntese - Apenas um servidor mantém as informações de todos.;
  - As consultas são feitas apenas no servidor central;
  - Exposto a estrangulamento de rede e a um ponto de falhas.

Caching

Intra-cluster

- Por Hashing:
  - Um servidor mantém uma função hashing com as informações da URL do conteúdo e endereços de IPs dos servidores da CDN;
  - Todos os pedidos são redirecionados;
  - Possui baixa complexidade de implementação;
  - Maior eficiência no compartilhamento de conteúdo.
- Por semi-Hashing:
  - Um servidor possui parte do seu armazenamento para a mesma função hashing do por Hashing;
  - Outra parte para cache dos conteúdos mais pedidos;
  - Cria 2 níveis de caches;
  - Voltado para armazenamento de conteúdo multimidia;
  - É o mais eficiente metódo de distribuição de conteúdo.

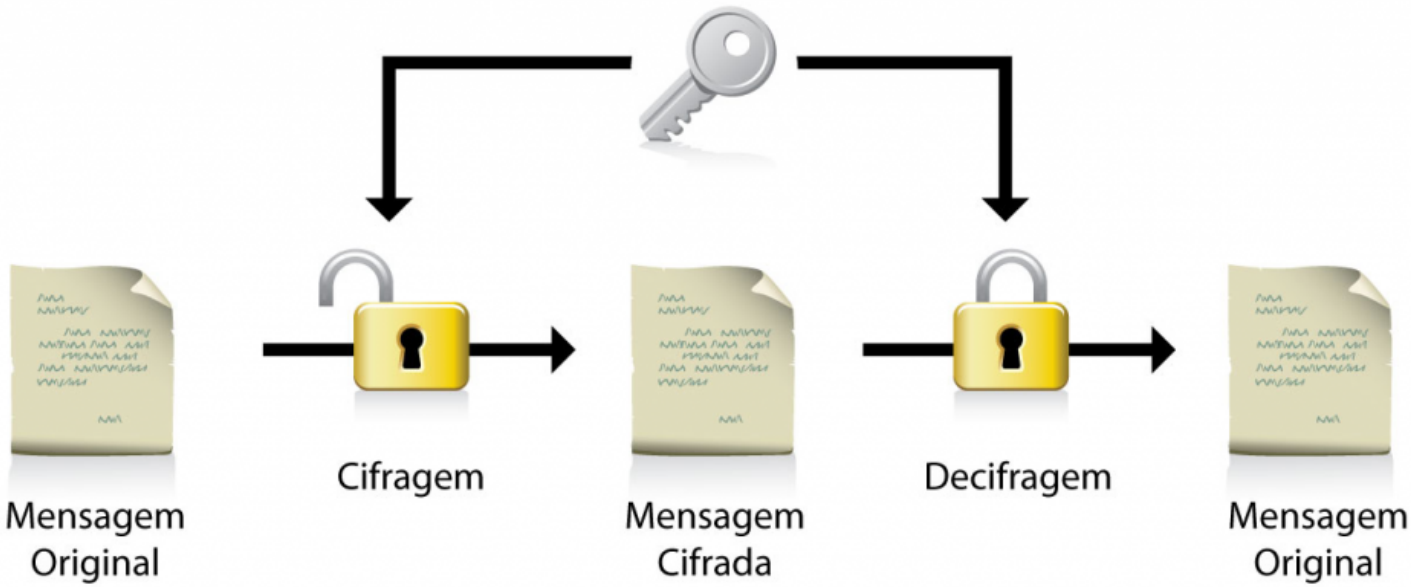
Sumário

Criptografia

Tipos de chaves

- Simétricas
- Assimétricas

Chaves simétricas



Chaves simétricas

Algoritmos mais consideráveis

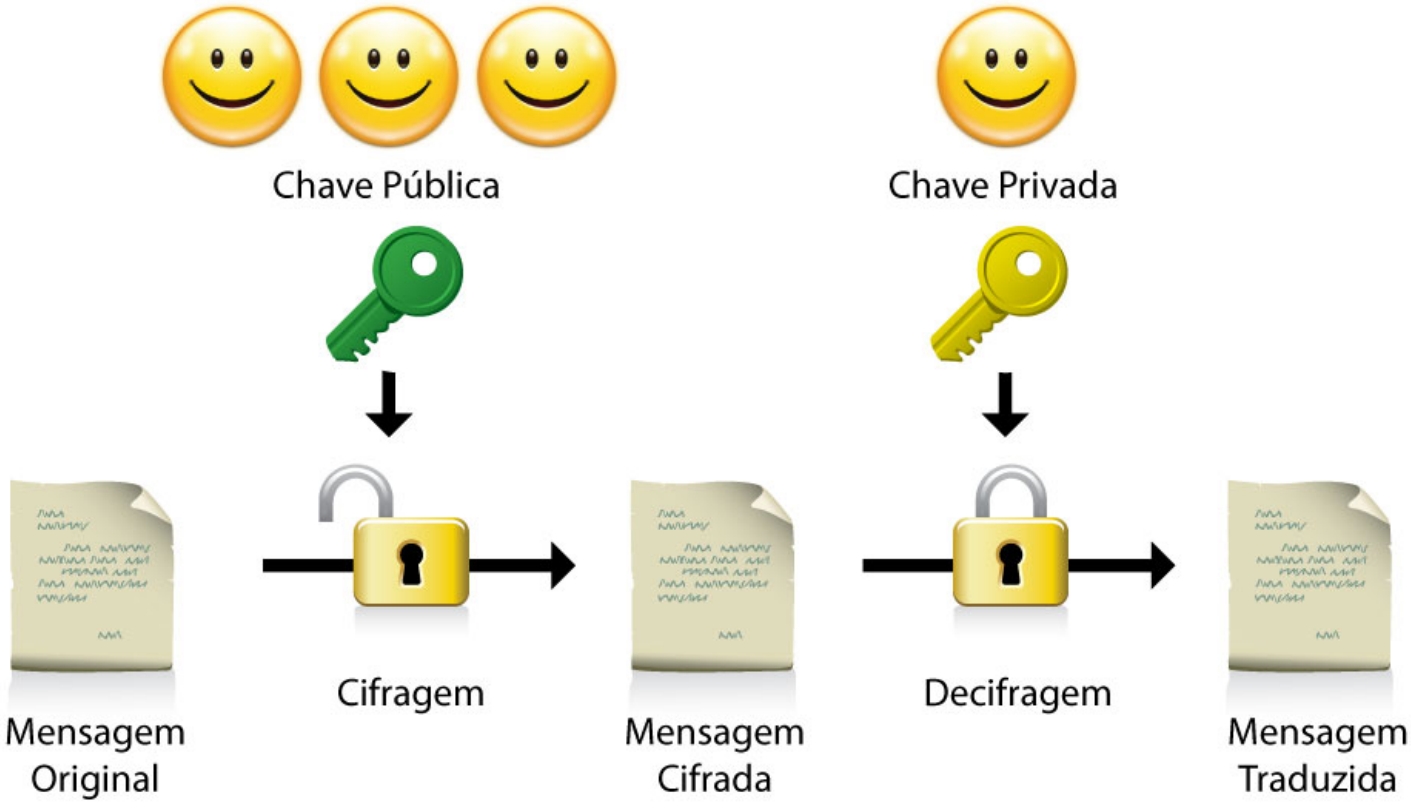
- Cifradores de Vernam;
- DES (Data Encryption Standard) - Usa chave de 56 bits;
- 3DES - Usa chave de 168 bits;
- AES (Advanced Encryption Standard) - Usa chave de 128, 192 ou 256 bits;
- A5/1, A5/2 e A5/3 - Criptografia de voz;

Chaves assimétricas

Acordo de chaves Diffie-Hellmann

O acordo de chaves Diffie-Hellmann permite estabelecer uma chave secreta comum entre duas entidades, mesmo usando canais de comunicao inseguros.

Chaves assimétricas



Chaves assimétricas

Aplicações

- git;
- ssh;
- Assinatura digital;
- Certificados digitais.
- entre outros.

VOD - Video On Demand

Proteção de conteúdo

Sumário

Autenticação de usuário

Em um sistema a autenticação de usuário pode se dar de 3 formas:

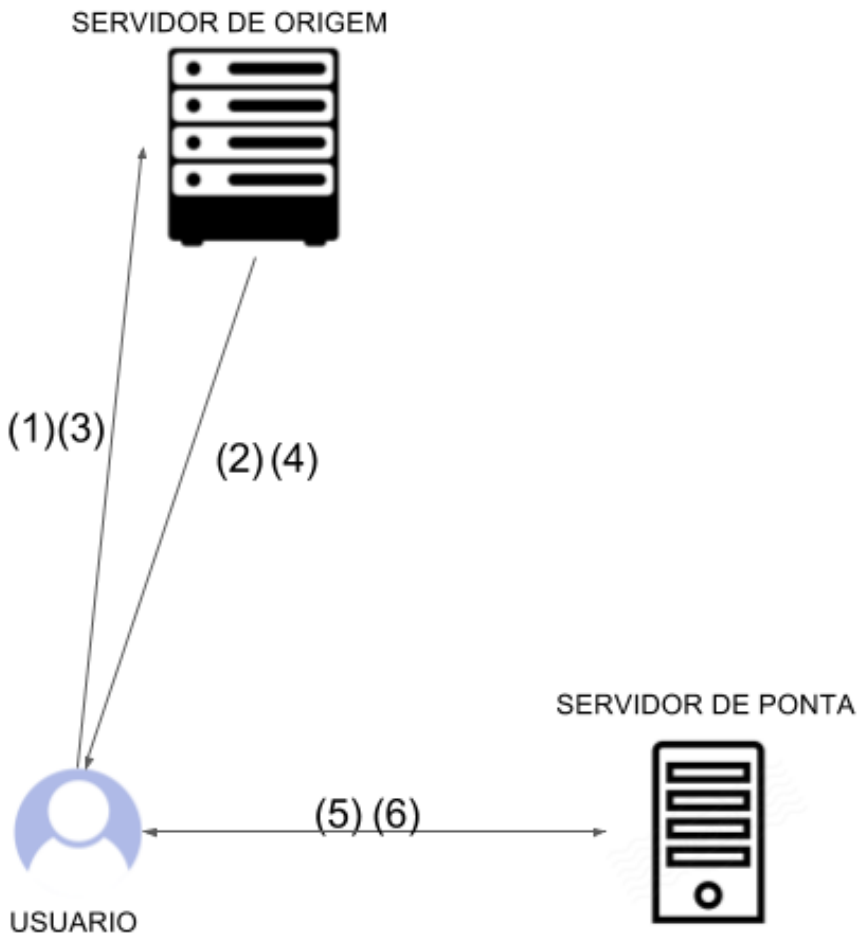
- **SYK Something You Know** - Algo que você SABE. Ou seja, um sistema de login/senha.
- **SYH Something You Have** - Algo que você TEM. Ou seja, um token, um smart card, um cartão magnético, um código de barras, etc.
- **SYA Something You Are** - Algo que você É. Ou seja, características intrinsecamente associada ao usuário.

Em uma CDN, exceto no protocolo SOCKS, o fornecedor do conteúdo pode escolher de qual forma vai proteger o seu conteúdo. Podendo alternar entre essses métodos ou até misturá-los.

IPTV

Autenticação de usuário

(1)	Faz login usando SYK
(2)	Recebe um user token
(3)	Envia um pedido com a URL do VOD
(4)	Recebe a URL do servidor de ponta mais perto
(5)	Envia um request com o user token
(6)	Recebe o conteúdo criptografado se tiver autorizado



References I