

# Autenticação e Autorização em Sistemas Web

Capítulo 3. HTTPS

Prof. Angelo Assis

# Autenticação e Autorização em Sistemas Web

---

Aula 3.1. Criptografia

Prof. Angelo Assis

# Nesta aula

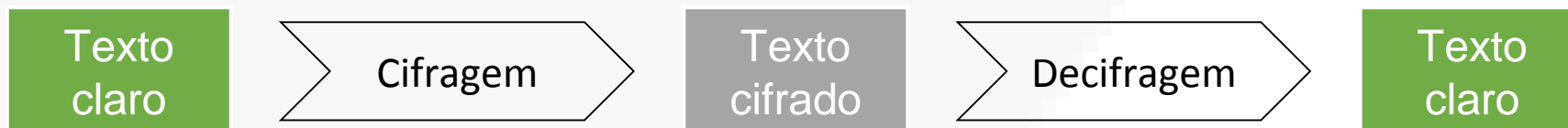


- ☐ Criptografia básica.
- ☐ Cifra de César.

# Criptografia



“É a ciência e a arte de manter mensagens seguras” - Bruce Schneier

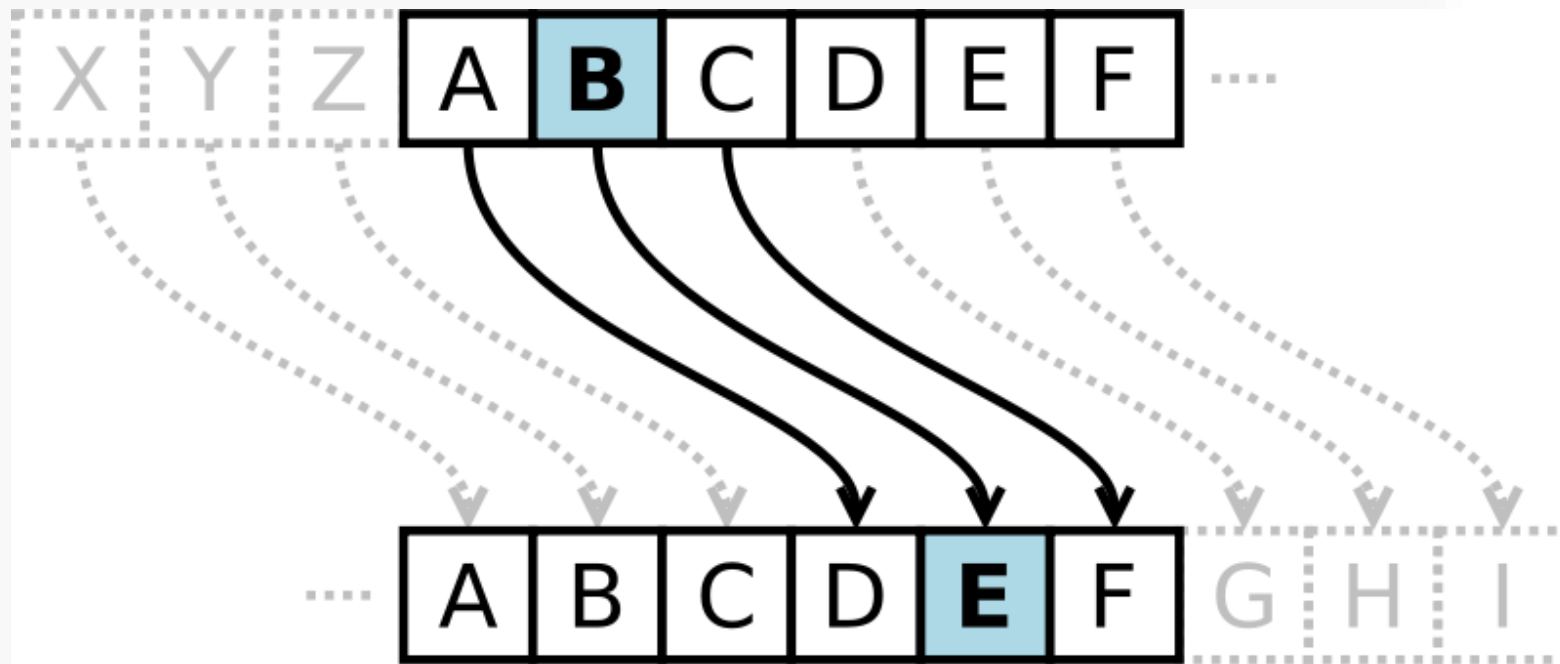


# Criptografia de chave simétrica



- Utiliza uma chave secreta e um algoritmo de criptografia.
- Criptografia e decriptografia são realizadas utilizando a mesma chave.
- “Ingredientes”:
  - Texto / Mensagem;
  - Algoritmo de criptografia;
  - Chave secreta;
  - Texto cifrado;
  - Algoritmo de decriptografia.

# Cifra de César



# Cifra de César



- “Chave = 3”:
  - OLA MUNDO → ROD PXQGR
- “Chave = 11”:
  - OLA MUNDO → ZWL XFYDZ
- Cifra de César “online”:
  - [https://eapps.tech/cifra\\_de\\_cesar/](https://eapps.tech/cifra_de_cesar/)

# Fraquezas



- Mensagem pode ser descoberta por tentativa e erro (força bruta):
  - No exemplo anterior: 26 tentativas;
- Deixa “impressão digital”:
  - Diminuem o número de tentativas.
- Língua portuguesa (Fonte: UFRJ)
  - 6 vogais: A, E, I, O, U, (Y) - 48.75 %
  - 5 consoantes de frequência alta: S, R, N, D, M - 29.12 %
  - 10 consoantes de frequência média: T, C, L, P, V, G, H, Q, B, F - 21.03 %
  - 6 consoantes de frequência baixa: Z, J, X, K, W - 1.10%



# Próxima aula



- ☐ Chave polialfabética.

# Autenticação e Autorização em Sistemas Web

---

Aula 3.2. Chave Polialfabética

Prof. Angelo Assis

# Nesta aula



- ☐ Chave polialfabética.

# Chave polialfabética



- Utiliza uma palavra em vez de apenas uma letra

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Mensagem: “Segurança é fundamental”
- Chave: “IGTI” (8, 6, 19, 8)
- Tradução  
“segu.ranc.aefu.ndam.enta.l”  
“akzc.zggk.ikyc.vjtu.mtmi.t”

# Chave polialfabética



## Vantagens:

- Menor impressão digital;
- Estabilidade de frequência;
- Chave suprema:
  - Comprimento da chave = comprimento da mensagem.

## Melhorias:

- Misturar idiomas;
- Adicionar camada de permutação.

# Próxima aula



- ❑ Algoritmo Diffie-Hellman.

# Autenticação e Autorização em Sistemas Web

---

Aula 3.3. Algoritmo Diffie-Hellman

Prof. Angelo Assis

# Nesta aula



- ❑ Algoritmo Diffie-Hellman.



# Troca de chaves Diffie-Hellman



- Baseado em princípios matemáticos:
  - Existem funções complexas, mas também existem funções fáceis de se calcular.
- Números primos dificultam “tentativa e erro”.
- Distribuição uniforme: 3 é a raiz primitiva de 17.

# Troca de chaves Diffie-Hellman



Base	Expoente	Resultado	Resto da divisão por 17
3	1	3	3
3	2	9	9
3	3	27	10
3	4	81	13
3	5	243	5
3	6	729	15
3	7	2187	11
3	8	6561	16
3	9	19683	14
3	10	59049	8
3	11	177147	7
3	12	531441	4
3	13	1594323	12
3	14	4782969	2
3	15	14348907	6
3	16	43046721	1
3	17	129140163	3

# Troca de chaves Diffie-Hellman



1. A e B acordam com os números **3** e **17**;
2. A escolhe um número secreto **15**:  
 $3^{15} \bmod 17 = 6.$
3. B escolhe um número secreto **13**:  
 $3^{13} \bmod 17 = 12.$
4. A e B trocam os resultados (**6** e **12**);
5. A calcula  $12^{15} \bmod 17 = 10$
6. B calcula  $6^{13} \bmod 17 = 10$

# Função de via única



- Hash
- Resultado de tamanho fixo
- Algoritmos SHA e MD5

# Próxima aula



- ❑ Criptografia de chave assimétrica.

# Autenticação e Autorização em Sistemas Web

---

Aula 3.4. Criptografia de Chave Assimétrica

Prof. Angelo Assis

# Nesta aula



- ❑ Criptografia de chave assimétrica.

# Chaves de Criptografia



- Chaves simétricas: Mesma chave encripta e decripta:
  - $E(c, m) = m'$
  - $D(c, m') = m$
  - Ideal para um único equipamento / usuário
- Chaves assimétricas: Uma chave encripta e outra decripta:
  - $E(c, m) = m'$
  - $D(c', m') = m$
  - Mais utilizado na internet
  - Chave  $c$  é pública
  - Chave  $c'$  é privada



# Chave assimétrica



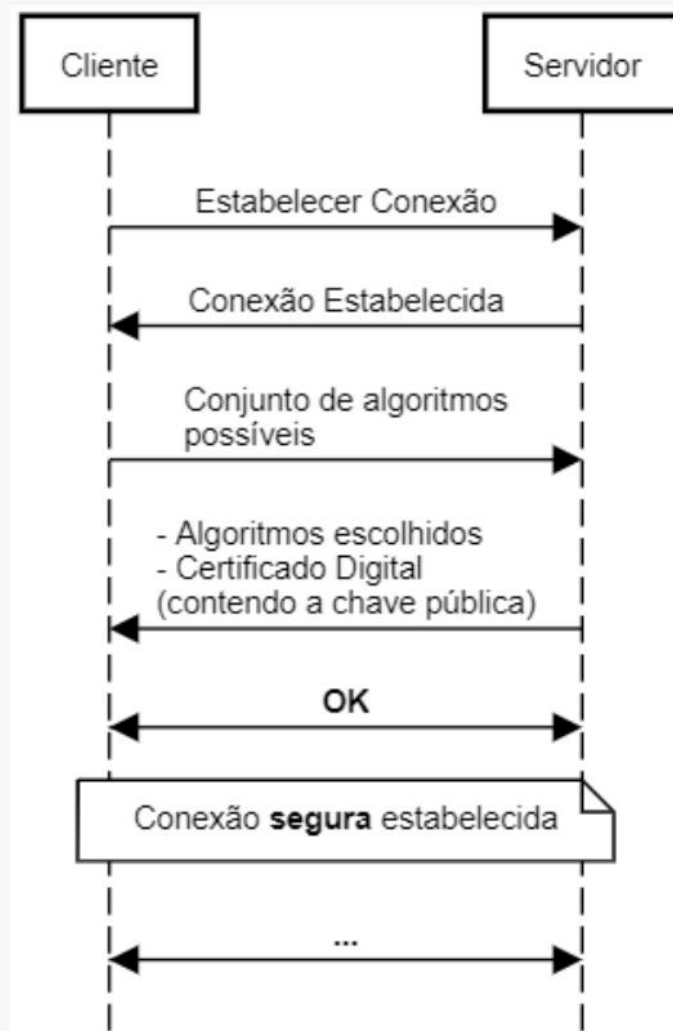
- Mensagem criptografada com chave pública do destinatário:
  - Somente o destinatário pode ler (Chave privada);
  - Conteúdo confidencial.
- Mensagem criptografada com chave privada do remetente:
  - Todos podem ler (Chave pública);
  - Assinatura:
    - Remetente.
- As chaves podem ser usadas em conjunto:
  - RSA, DAS.

# TLS



- Criptografia
  - Chaves simétricas
  - Chaves assimétricas
  - Hash
- Partes negociam
  - Algoritmos
  - Chaves
  - Parâmetros
- Servidor toma a decisão final

# TLS



# TLS



- Protocolo
  - TLS 1.1, 1.2, 1.3, SSL
- Troca de Chaves
  - Diffie-Hellman, RSA
- Algoritmo de Criptografia
  - AED, DES
- Certificado
  - Garantir confiabilidade do destinatário

# Conclusão



✓ HTTPS é o protocolo HTTP combinado com TLS.

# Próxima aula



- ❑ Certificado Digital.

# Autenticação e Autorização em Sistemas Web

---

Aula 3.5. Certificado Digital

Prof. Angelo Assis

# Nesta aula



- ☐ Certificado Digital.



# Certificado Digital



Como confiar na outra parte?


# Certificado Digital



- Documento digital.
- Informações:
  - Entidade certificada;
  - Validade;
  - Chave pública;
  - Assinatura digital;
  - Autoridade Certificadora (AC).

# Certificado Digital








**A conexão é segura**



Suas informações (por exemplo, senhas ou números de cartão de crédito) permanecem privadas quando são enviadas para esse site. [Saiba mais](#)

---


 **Certificado** (válido)

 **Cookies:** (96 em uso)

 **Configurações do site**

 **Certificado** 

**Geral** Detalhes Caminho de Certificação

 **Informações sobre o Certificado**

---

**Este certificado destina-se ao(s) seguinte(s) fim(ns):**

- Prova a sua identidade para um computador remoto
- Garante a identidade de um computador remoto
- 2.16.840.1.114412.1.2
- 2.23.140.1.2.1

\* Veja a declaração da autoridade de certificação para obter d

---

**Emitido por:** www.globo.com

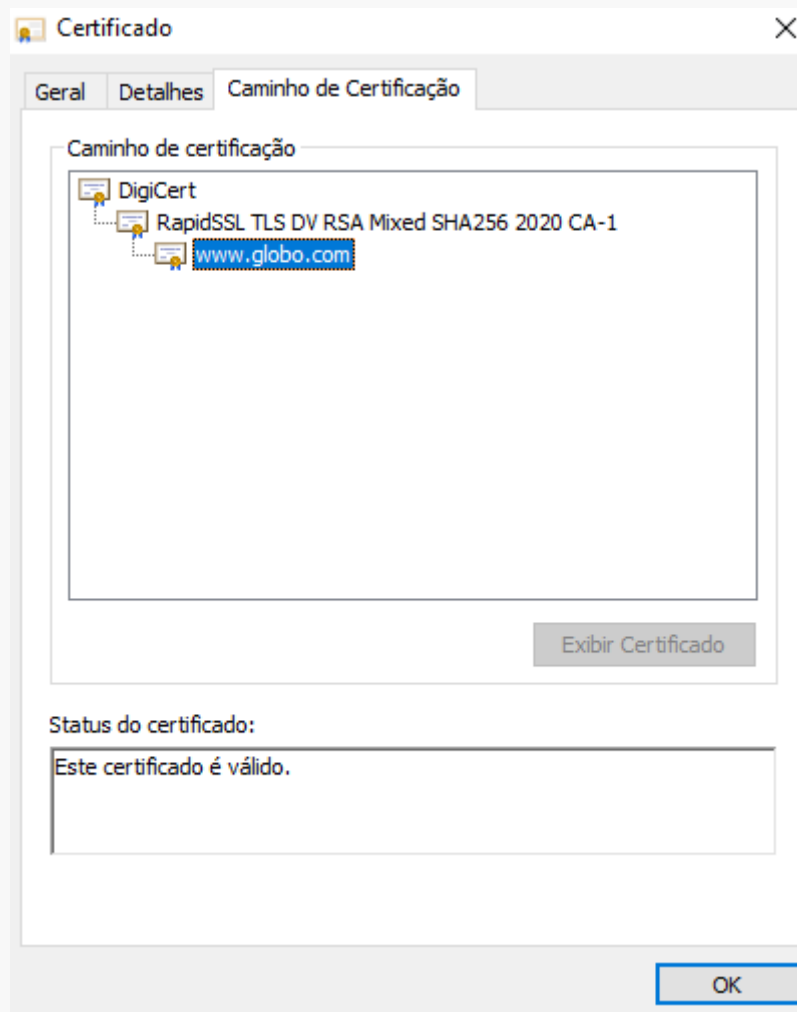
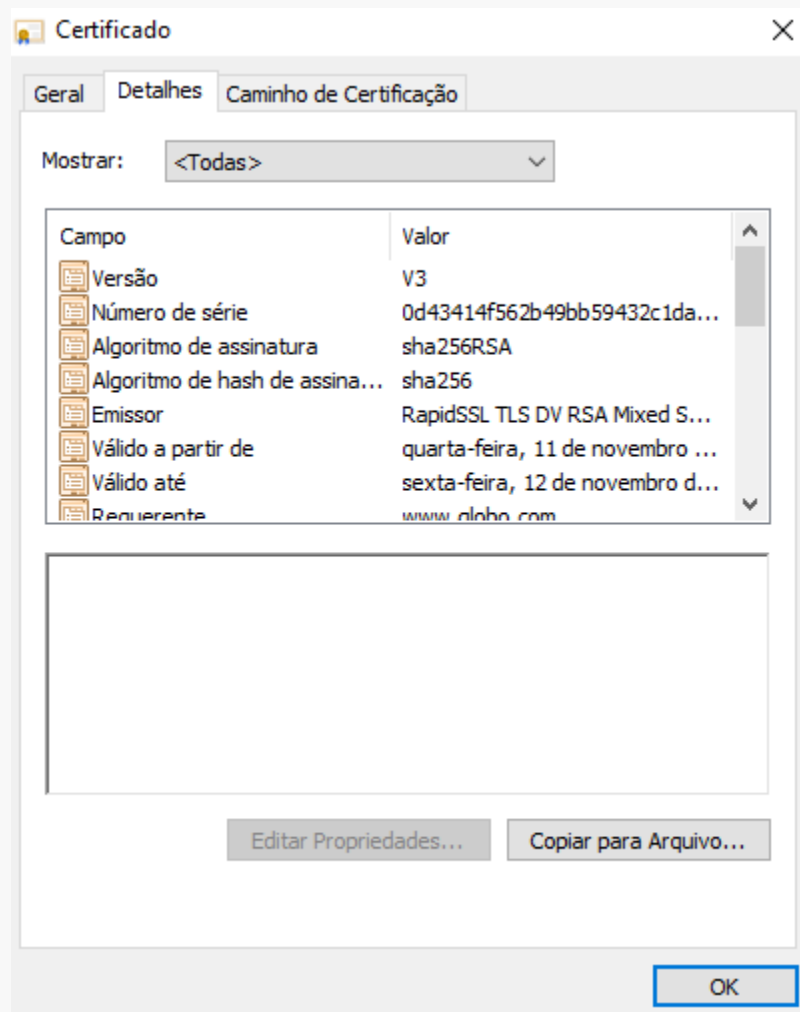
**Emitido por:** RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1

**Válido a partir de** 11/11/2020 **até** 12/11/2021

**Declaração do Emissor**

**OK**

# Certificado Digital





# Certificado Digital – Brasil



- SERPRO.
- Caixa Econômica Federal.
- Serasa.
- Receita Federal.
- Prodemge.
- Outros.

# | Próxima aula



- ❑ Oauth 2.0.