

# Pilares da Segurança e Chaves criptográficas

Marcus Botacin<sup>1</sup>

<sup>1</sup>Assistant Professor  
Texas A&M University (TAMU), USA  
botacin@tamu.edu  
@MarcusBotacin

# Tópicos

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia

- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia

- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

# As Propriedades da Segurança: Introdução

## Propriedades ACID

- Autenticidade
- Confidencialidade
- Integridade
- Disponibilidade

# As Propriedades ACID

## Autenticidade

- Quem é você?
- Você é você mesmo?

## Onde você vê:

- Formulários de *login*.
- Autenticação por chaves.

## Não confundir com: Autorização

- Você pode fazer isso?

# As Propriedades ACID

## Confidencialidade

- Apenas as partes sabem sobre isso?
- Nenhum terceiro pode ficar sabendo sobre isso?

## Onde você vê:

- Formulários de submissão criptografados.
- Conexões encriptadas.

## Não confundir com: Anonimidade

- Ninguém sabe quem você é!

# As Propriedades ACID

## Integridade

- Os dados são o que deviam ser?
- Os dados continuam como estavam?

## Onde você vê:

- Permissões de leitura/escrita.
- Controles de acesso.
- Soluções de backup.

## Quando é violado:

- Ataques por *Ransomware*

# As Propriedades ACID

## Disponibilidade

- Eu ainda consigo acessar os dados?
- Quando eu precisar, os dados estarão lá?

## Violações de Disponibilidade: Onde você vê:

- Eventos tipo *Black Friday* (benigno)
- Ataques do tipo Negação de Serviço (DoS) (malicioso)

# As Propriedades da Segurança: Resumo

## Propriedades ACID

- Autenticidade
- Confidencialidade
- Integridade
- Disponibilidade

## Propriedades Derivadas

- Privacidade
- Anonimidade
- Não-Repúdio

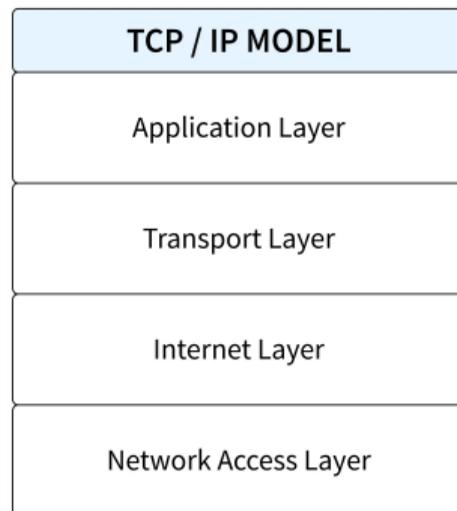
# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia

- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

# Onde vai a segurança?

## A Pilha TCP/IP



# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - **Criptografia**

- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

# O Problema: Man-In-The-Middle

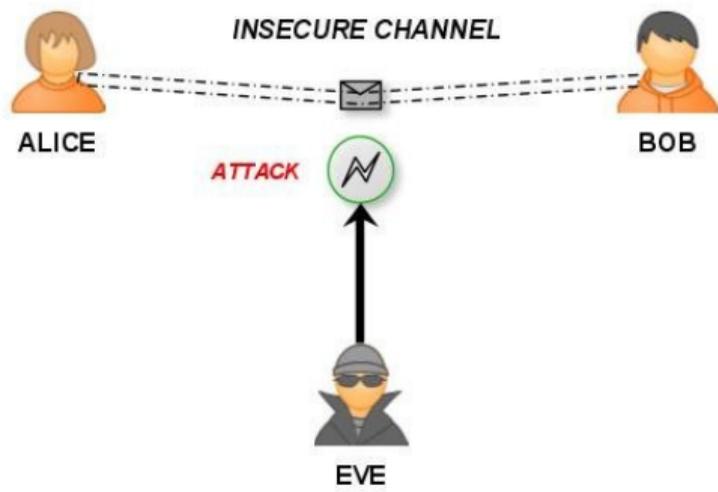


Figure: Fonte: <https://tinyurl.com/5dekpu74>

# A Solução: Criptografia

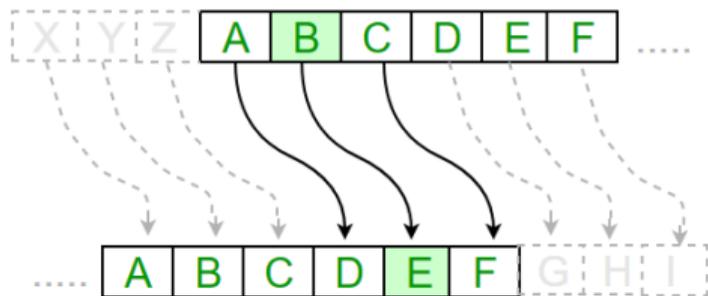


Figure: Fonte: <https://tinyurl.com/df8ubpht>

## Caesar, Shift the Cipher

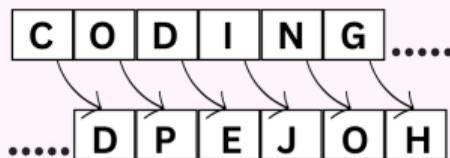


Figure: Fonte: <https://tinyurl.com/mrx8p3ms>

# Criptografia “de verdade”

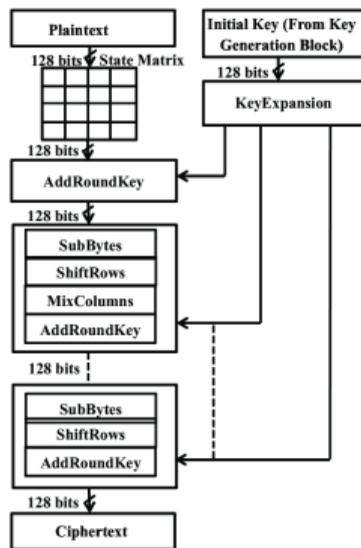


Figure: Fonte: <https://tinyurl.com/3zjnremx>

# Criptografia de Chave Simétrica

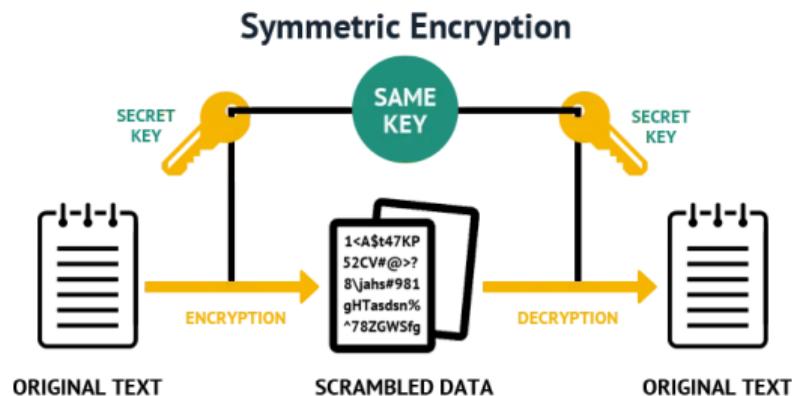


Figure: Fonte: <https://tinyurl.com/mttstkmv>

# Criptografia de Chave Assimétrica

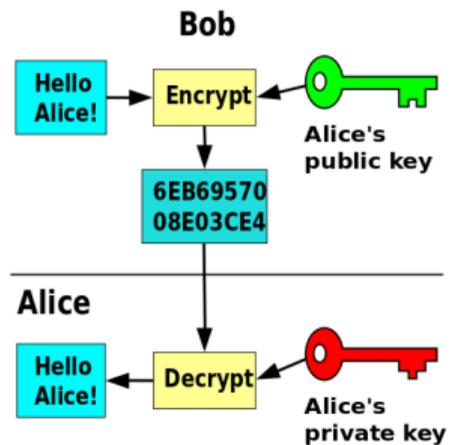


Figure: Fonte: <https://tinyurl.com/yb4956rc>

# Negociação de Chaves

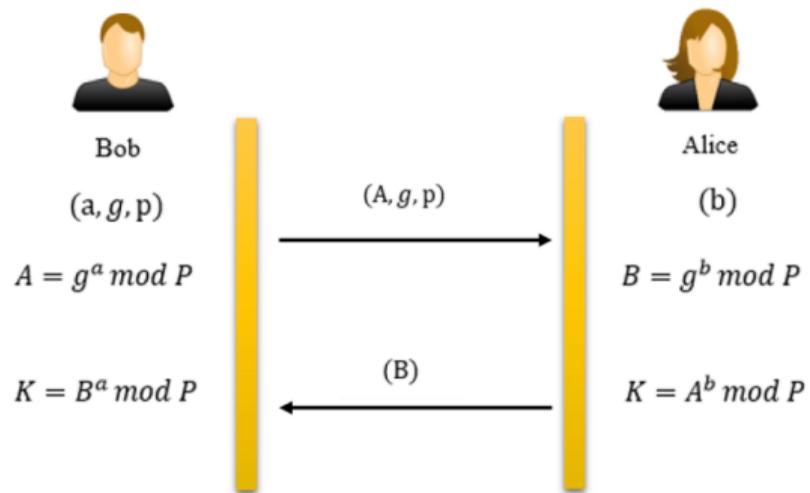


Figure: Fonte: <https://tinyurl.com/y6pm592m>

Figure: Video: <https://youtu.be/qgzpJnStGto>

# Resumo

## Tipos de Criptografia

- Simétrica: Onde todas as partes utilizam a mesma chave.
- Assimétrica: Onde as partes utilizam chaves diferentes.

## Criptografia Assimétrica: Tipos de Chaves

- Pública: A chave visível no canal inseguro.
- Privada: A chave mantida sob controle exclusivo da parte.

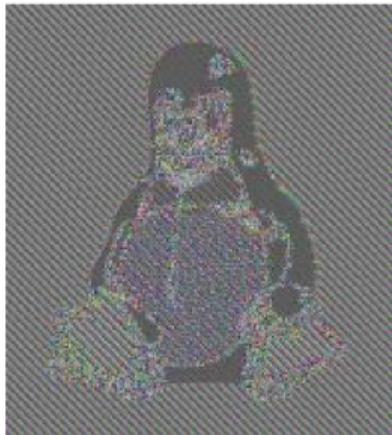
## Criptografia na Internet

- 1 Estabelecimento de chave via Diffie-Hellman.
- 2 Troca de dados via chave simétrica compartilhada.

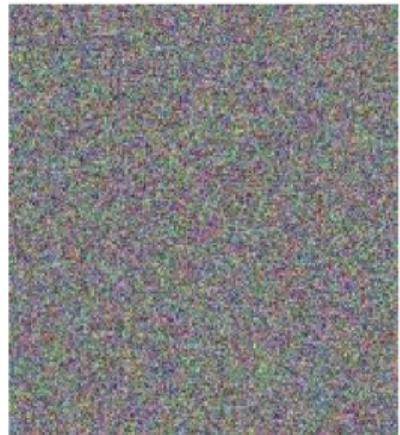
# Desafio: Configuração Adequada



(a) Original image



(b) Encrypted with AES only



(c) Encrypted with AES using CBC mode

Figure: Fonte: <https://tinyurl.com/39ezvxf5>

# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia

- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

# Publicação

RESEARCH-ARTICLE



## The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Authors [Marcus Botacin](#) [Anatoli Kalysch](#) and [André Grégio](#) | [Authors Info & Claims](#)

*ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security* • August 2019  
Article No.: 49, Pages 1 - 10 • <https://doi.org/10.1145/3339252.3340103>

**Published** 26 August 2019 [Publication History](#)



2 421



Figure: Fonte: <https://dl.acm.org/doi/10.1145/3339252.3340103>

# Man-In-The-Middle (Banco 1)

```
Flow Details
2018-11-15 20:34:42 POST https://200.201.160.36/sinbc/nb/loginLight?nocache=1542321254170&ciphredKey=YAYMHVP1hA9kfsdtl548
vqxLgHig0gSTVInbjYvRuiQmk-
← 200 OK text/html 56.67k 1.62s

Request Response Detail
<div id="textoLogin" class="hidden-xs">
<p class="titlePanels titleLogin">JÁ SOU USUÁRIO DO</p>
<p class="titlePanels titleLoginIBC">INTERNET BANKING CAIXA</p>
</div>
<div class="titleLoginXS2 hidden-sm hidden-md hidden-lg" style="text-align: center; font-weight:
bold;">IDENTIFICAÇÃO DO USUÁRIO</div>
<div class="descLoginBloc clearfix">
<form id="user" action="/sinbc/nb/loginLight?nocache=1542321254170& ciphredKey=YAYMHVP1hA9kfsdtl548vqxLgHig0
gSTV1NbjYvRuiQmk0IgwCbFLABVigPpxftlodr7dxLGTMJ%2F5AWBu0In8AJSjzfzC9zIGfEgxxKigK5ed33hVnCIeM2Wq3oGchdTaf7RLAMkyqEV1%2FCBazI
prxMYbr7xQen%2FmRzxCCKLZdIX3D8&ciphredId=FDqCmApHue5%2Fcd230nI3NbR0T543%2FPL%2BUPXBCttGVUBY23sa9mAdy19x%2FqKUJQ9oIdTFZ
CTvLExJmMwXDo092BCWw4wxSxTR5CQaU5B07nJlTBMx%2B7YxmpVxzPx3UCITUE1BYZH8FOVvFU%2F0zHu8aUsvfH0F0515yeSjuwJsaDqXXUYJ0VKen%2FWwz
NsnRajXpBNW9i0MtoTfmsNGSebQ5bLgWtl%2F250uoz9WoxTgYFivxHDY1%2FQIv1vUZBwmq2hka8x45Z62%2FbQk2xgC09GU3zH17tM0aqGDxzRYC7wJyNuvS
U0e%2BJxk1dCyp03Gp736Uz6NnxtLbBF%2F%2FhFhhSzbHpUhf%2Bp94ZmsSZ5Ll9yukFZtXuCmTnJWIsaN0i70ci2yoZfH8GJyHEc%2FUEL7IjMgWHEt9tY
fbjUo8CVq0oQAJUS4ctbtkG7KL7Jlhf0Pfmznzh7kyBPy%2FLOVEKAB7FmLRdce471jEh1lBfW7VpV1TbB8FcdNdx80fGLRMgh8x%2FeA7R0KpSmuY6LtiVp
%2BJ1HX3hLtaAY%2Fq7caPjF2hs5a5fePCX2B6DI%2Fw0aumvz28b7YfSvvpZM8IFe4rq1YhrEQMoPRX2u4DyC92W9V7Ql8U%3D&amo;SO=11& ;SOVersao
=5.1& ;AppVersao=3.3.4& ;fresh=1" method="POST">
<input type="hidden" name="infoCmdWS" id="infoCmdWS" value="" />
<input type="hidden" name="f10CndWS" id="f10CndWS" value="" />
<input type="hidden" name="digestWS" id="digestWS" value="" />
<input type="hidden" name="siglaWS" id="siglaWS" value="" />
<input type="hidden" name="idWS" id="idWS" value="" />
<input type="hidden" name="seedWS" id="seedWS" value="" />
<input type="hidden" name="warsawIEWindows" id="warsawIEWindows" value="" />
<input type="hidden" name="warsawInstalled" id="warsawInstalled" value="" />
↓ [2/56] [transparent] [*:8080]
```

# Man-In-The-Middle (Banco 2)

```
Flow Details
2018-11-15 20:44:24 POST https://54.232.239.132/api/proxy/AJxL5LApUvAX0b5R5DnjMw3-9lbnk8UnZg.aHR0cHM6Ly9wcm9kLWdsb2JhbC1hd
XRoLm51YmFuay5jb20uYnIvYX...
← 401 Unauthorized application/json 24b 779ms

Request Response Detail
Cache-Control: no-cache
user-agent: Android/5.23.13-minApi21-20487 (7391db29fe31986f; 5.1; asus; ASUS_Z00VD)
X-Correlation-Id: and-5_23_13-minApi21-20487.jslyt
Accept-Encoding: gzip
X-Device-Id: 7391db29fe31986f
Content-Type: application/json; charset=UTF-8
Content-Length: 1057
Host: prod-s0-webapp-proxy.nubank.com.br
Connection: Keep-Alive

JSON [a:auto]
{
  "device_id": "7391db29fe31986f",
  "login": "95430119822",
  "model": "Asus ASUS_Z00VD",
  "password": "12345678",
  "public_key": "----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzJtL0Cc+8MrKnJkc6oV\n8/Tja/6ee
k3PyJNaoENZG9CFm9H2TatXGz9qdH9KV002F5EIVt04EEr5qfidz/K\nnFPCNictE7Xoh4AkGw0KY0+o5SC0S6x0pARoxDd2Xqaqr/kI+0LvtAaril1GF0Q\
n3wq4zIx+U0AuvGrkK5sGbnunmHh5d3Yt8/G6b2VPLJhJl8lqrBaN2vosY+kvuTF\nnRgzi208oJshNVN6sYDz1TS9GOLCw9QgY9sDPBRsruv/JzD2KUqXKj2q
jY8QUHQPV\nv260AEK33AeGIKJaSvxh6Cvjg51PuQA1j3XpFKo0w/9005KgN0T2DTqbz2zYDY0n\nnxQIDAQAB\n-----END PUBLIC KEY-----",
  "public_key_crypto": "----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAEuzGEhG3g3rSg0r6S8bMq\n8ZrQNDN6EahJ53ZLpYNTCKplagoSj8/3CCSEawS0DIXDOW50GgFlqnMeYsMeU60n\ns fakaz03KP5n8yZdSIHGR96bvCgefmrR4cz7zIH1WlZPDT5d23fjEZ0i4i0
Bvk1FQ\nnfMwUzmrE7Z7NJBx0x5nqaDzKDF22diQ5L8Au5L0JN0wsgLVMSuP07Rl9W1qCgdT\nnverBZ0rrw9gcvzDtKTD+6d18otljNRFuweKx3hHD50bzLhz6
downxzd8stUkAbxx\nnYGT99Q3pY/ARenZGMR/ulWihgF/sCBQsoSPOV4/5ZGsJ5uPxnF0m8Htb0HMMq335\nnJQIDAQAB\n-----END PUBLIC KEY-----"
}
```

# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia

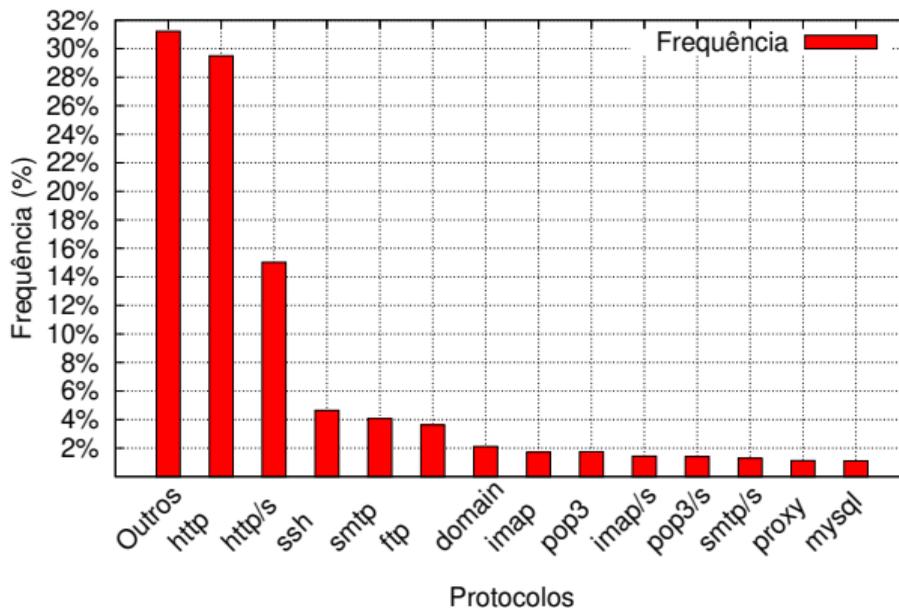
- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 Conclusões
  - Conclusões

The image is a screenshot of an arXiv preprint page. At the top left, the arXiv logo is displayed in white on a dark red background, followed by the breadcrumb path '> cs > arXiv:2109.06068'. To the right of this path is a search bar with the placeholder text 'Search...'. Below the breadcrumb path, the text 'Help | Adv' is partially visible. The main content area has a light gray background. It starts with the category 'Computer Science > Cryptography and Security'. Below this, the submission date is noted as '[Submitted on 13 Sep 2021]'. The title of the preprint is 'A [in]Segurança dos Sistemas Governamentais Brasileiros: Um Estudo de Caso em Sistemas Web e Redes Abertas', displayed in a large, bold, black font. Below the title, the authors' names 'Marcus Botacin, André Grégio' are listed in a smaller, blue font.

Figure: **Fonte:** <https://arxiv.org/abs/2109.06068>

# Escaneamento do domínios .gov

Distribuição dos Protocolos



# Possíveis Falhas de Segurança (1/2)

```

[redacted]:~/dominios/scans$ dig @ [redacted].gov.br google.com
; <<>> DiG 9.10.3-P4-Ubuntu <<>> @ [redacted].gov.br google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6764
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                273     IN      A      172.217.29.174

;; AUTHORITY SECTION:
google.com.                7134    IN      NS     ns3.google.com.
google.com.                7134    IN      NS     ns2.google.com.
google.com.                7134    IN      NS     ns1.google.com.
google.com.                7134    IN      NS     ns4.google.com.
```

## Possíveis Falhas de Segurança (2/2)

```
[redacted]:~/dominios/scans$ nc [redacted].gov.br 25  
220 [redacted].gov.br ESMTP Postfix  
MAIL FROM: i_am@intruder.com  
250 2.1.0 Ok
```

# Agenda

- 1 O que é estar seguro?
  - Conceitos
  - Segurança na Internet
  - Criptografia
- 2 Quando a segurança falha
  - Aplicativos Bancários
  - Sistemas Governamentais
- 3 **Conclusões**
  - **Conclusões**

# Resumo

## Problema

- Os protocolos de Internet não foram projetados com segurança em mente.

## Solução

- Soluções de segurança propostas na camada de aplicação: e.g., Criptografia.

## Desafio

- 1 Configuração adequada de serviços e protocolos criptográficos.

Obrigado!  
Dúvidas? Comentários?  
botacin@tamu.edu  
@MarcusBotacin