Técnicas Criptográficas

MiEI, MiEBM

Óscar Pereira

oscar@di.uminho.pt

Uminho, EEng, DI (Gualtar)

1º semestre – 2020/21

Semana 02

Covid...

E não esquecer ligar o bluetooth...

Criptografia Simétrica — Katz e Lindell, cap. 3

Mas antes disso...

Criptografia Simétrica — Katz e Lindell, cap. 3

Mas antes disso...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Princípios de Criptografia Moderna

Katz e Lindell, cap. 1

- ***Kerckhoff:*** O inimigo sabe **tudo**, excepto a ***chave!***
- ***Definições formais:*** precisão, em vez de ideias difusas
- ***Pressupostos rigorosos***
- ***"Provas de Segurança..."***

Vamos ver cada uma em mais detalhe...

Principio I — **Definições formais**

- "Fazer bem feito" vs. "fazer o que tem que ser feito"
- Definições ***rigorosas***
- Problema da ***axiomática:*** a definição captura realmente o que é suposto?
- Ou seja, formalismos: úteis, mas limitados
- Exemplo: Vigenère para mensagens curtas?

Principio I — **Definições formais**

- "Fazer bem feito" vs. "fazer o que tem que ser feito"
- Definições ***rigorosas***
- Problema da ***axiomática:*** a definição captura realmente o que é suposto?
- Ou seja, formalismos: úteis, mas limitados
- Exemplo: Vigenère para mensagens curtas?

Principio I — **Definições formais**

- "Fazer bem feito" vs. "fazer o que tem que ser feito"
- Definições ***rigorosas***
- Problema da ***axiomática:*** a definição captura realmente o que é suposto?
- Ou seja, formalismos: úteis, mas limitados
- Exemplo: Vigenère para mensagens curtas?

Principio I — **Definições formais**

- "Fazer bem feito" vs. "fazer o que tem que ser feito"
- Definições ***rigorosas***
- Problema da ***axiomática:*** a definição captura realmente o que é suposto?
- Ou seja, formalismos: úteis, mas limitados
- Exemplo: Vigenère para mensagens curtas?

Principio I — **Definições formais**

- "Fazer bem feito" vs. "fazer o que tem que ser feito"
- Definições ***rigorosas***
- Problema da ***axiomática:*** a definição captura realmente o que é suposto?
- Ou seja, formalismos: úteis, mas limitados
- Exemplo: Vigenère para mensagens curtas?

Principio I — **Definições formais**

Normalmente consistem em duas partes:

- Garantia de segurança: o que significa **atacar com sucesso**?
- "Threat model:" o poder de que dispõe o atacante

Principio I — **Definições formais**

Normalmente consistem em duas partes:

- Garantia de segurança: o que significa **atacar com sucesso**?
- "Threat model:" o poder de que dispõe o atacante

Principio I — **Definições formais**

Normalmente consistem em duas partes:

- Garantia de segurança: o que significa **atacar com sucesso**?
- "Threat model:" o poder de que dispõe o atacante

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio II — **Pressupostos rigorosos**

- Porque pressupor o que quer que seja?! Limitações da teoria...
- Defini-los com rigor ajuda a ***estudá-los***
- Defini-los com rigor ajuda a **compará-los**
- Defini-los com rigor ajuda a **compreender o que é preciso**

Principio III — **Provas de segurança...**

- Outra coisa com o nome errado...
- Na realidade, são ***reduções***
- Reduzem a segurança da construção / protocolo...
- ... à segurança do(s) pressuposto(s) base

Principio III — **Provas de segurança...**

- Outra coisa com o nome errado...
- Na realidade, são ***reduções***
- Reduzem a segurança da construção / protocolo...
- ... à segurança do(s) pressuposto(s) base

Principio III — **Provas de segurança...**

- Outra coisa com o nome errado...
- Na realidade, são ***reduções***
- Reduzem a segurança da construção / protocolo...
- ... à segurança do(s) pressuposto(s) base

Principio III — **Provas de segurança...**

- Outra coisa com o nome errado...
- Na realidade, são ***reduções***
- Reduzem a segurança da construção / protocolo...
- ... à segurança do(s) pressuposto(s) base

Principio III — **Provas de segurança...**

- Outra coisa com o nome errado...
- Na realidade, são ***reduções***
- Reduzem a segurança da construção / protocolo...
- ... à segurança do(s) pressuposto(s) base

Segurança Computacional

Obrigado pela atenção!

Dúvidas