A beleza matemática da criptografia

Marcel de Sena Dall'Agnol

Como construir cripto?

(Não precisa de computador!)

Como construir cripto?

(Não precisa de computador!)

Objetivos (*threat modeling*):

- Confidencialidade
- Autenticação
- Integridade
- ...

Como construir cripto?

(Não precisa de computador!)

Objetivos (*threat modeling*):

- Confidencialidade
- Autenticação
- Integridade
- ...

Um componente básico: operação fácil de fazer, mas difícil de desfazer sem uma "chave".

Cifra de César

GENERAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HENERAL, ATAQUE AMANHÃ À
MEIA NOITE.

Cifra de César

HFNERAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOERAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFRAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BTAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUAQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUBQUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUBRUE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUBRVE AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUBRVF AMANHÃ À MEIA NOITE.

Cifra de César

HFOFSBM, BUBRVF BNBOIB B NFJB OPJUF.

Cifra de César

HFOFSBM, BUBRVF BNBOIB B NFJB OPJUF.

A	B	C	D	E	F	G	H	I	J	K	L	M
B	C	D	E	F	G	H	I	J	K	L	M	N
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Cifra de César

GENERAL, ATAQUE AMANHÃ À
MEIA NOITE.

Cifra de César

KIRIVEP, EXEUYI EQERLE E QIME RSMXI.

A	B	C	D	E	F	G	H	I	J	K	L	M
E	F	G	H	I	J	K	L	M	N	O	P	Q
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D

Cifra de Substituição

GENERAL, ATAQUE AMANHÃ À MEIA NOITE.

Cifra de Substituição

□∅▽∅#⊥■,

⊥Θ⊥∀Ω∅ ⊥ Γ∅∃⊥ ▽¬∃Θ∅.

A	B	C	D	E	F	G	H	I	J	K	L	M
⊥	♣	♠	§	∅	★	□	△	∃	♢	♡	■	Γ
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
▽	¬	▼	∀	#	Ξ	Θ	Ω	Π	ℵ	℧	Ⅎ	∠

O que significa ”difícil”?

Codificação binária

A = ○●○○○○○●

B = ○●○○○○●○

C = ○●○○○○●●

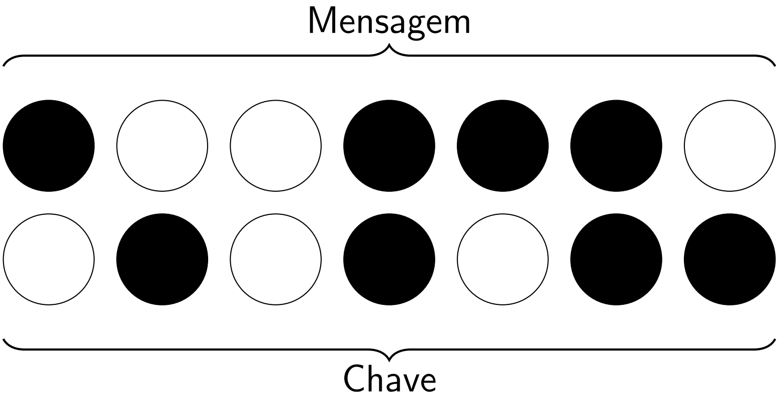
D = ○●○○○●○○

E = ○●○○○●○●

F = ○●○○○●●○

⋮

One-Time Pad (OTP)



XOR

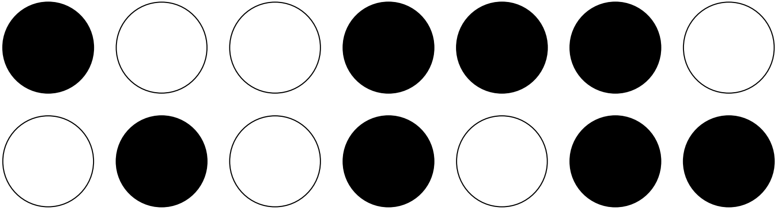
○ + ○ = ○

○ + ● = ●

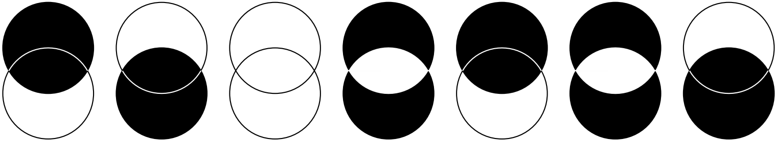
● + ○ = ●

● + ● = ○

One-Time Pad (OTP)



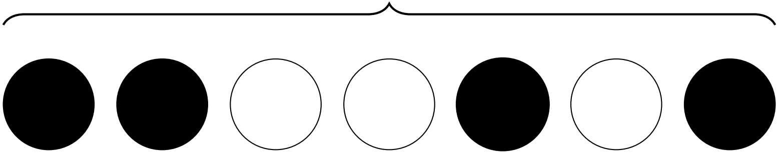
One-Time Pad (OTP)



One-Time Pad (OTP)

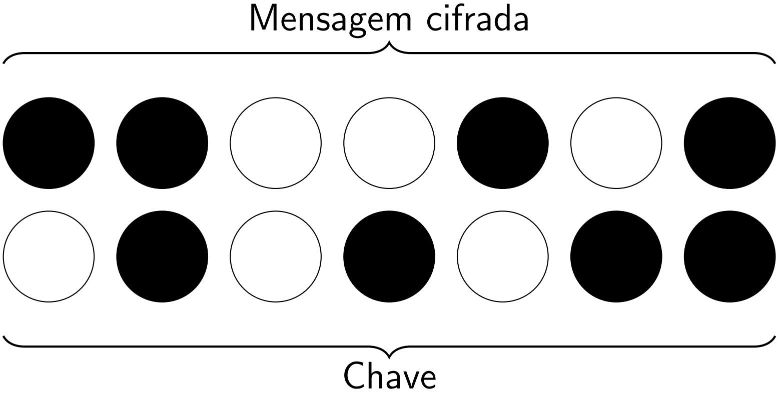
● ● ○ ○ ● ○ ●

One-Time Pad (OTP)



Mensagem cifrada

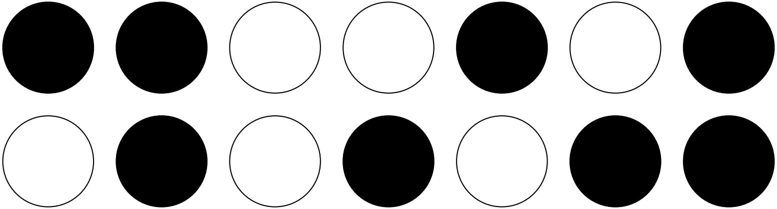
One-Time Pad (OTP)



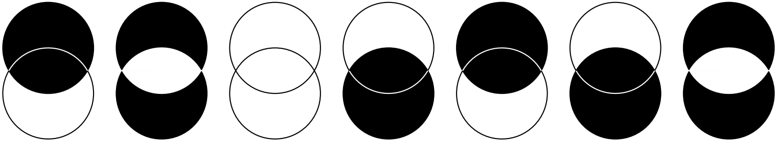
Mensagem cifrada

Chave

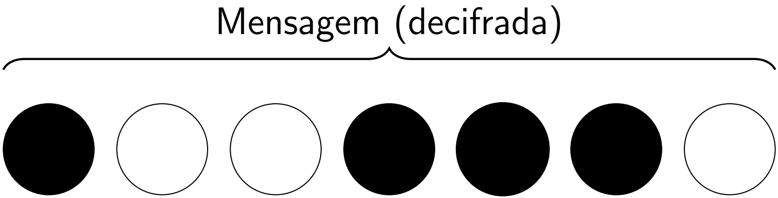
One-Time Pad (OTP)



One-Time Pad (OTP)



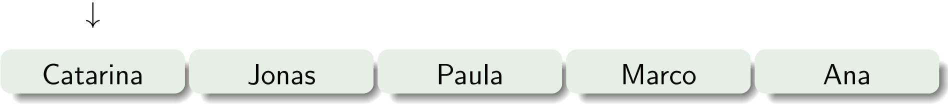
One-Time Pad (OTP)



Mensagem (decifrada)

Busca linear

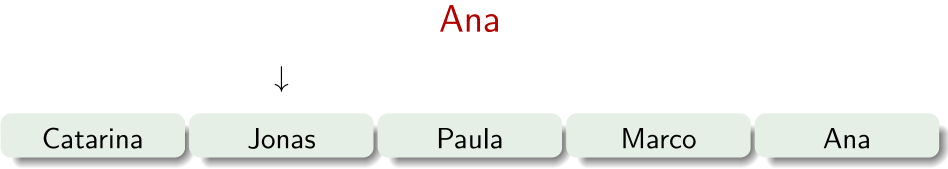
Ana



↓

Catarina | Jonas | Paula | Marco | Ana

Busca linear

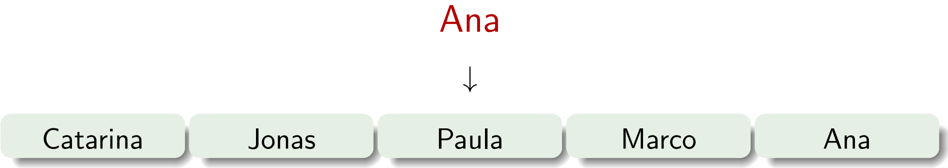


Ana

↓

Catarina Jonas Paula Marco Ana

Busca linear

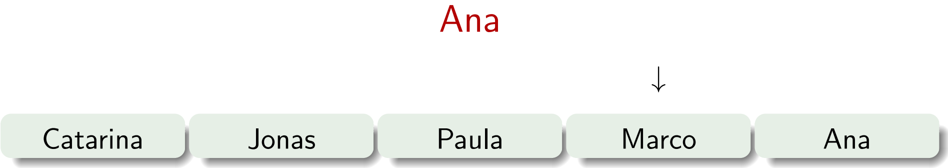


Ana

↓

Catarina | Jonas | Paula | Marco | Ana

Busca linear



Ana

↓

Catarina

Jonas

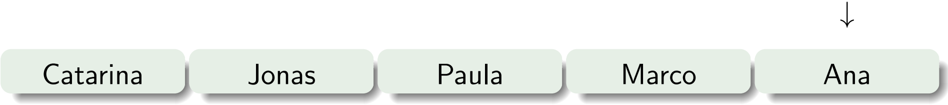
Paula

Marco

Ana

Busca linear

Ana

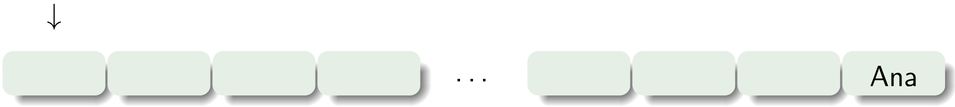


↓

Catarina Jonas Paula Marco Ana

Busca linear

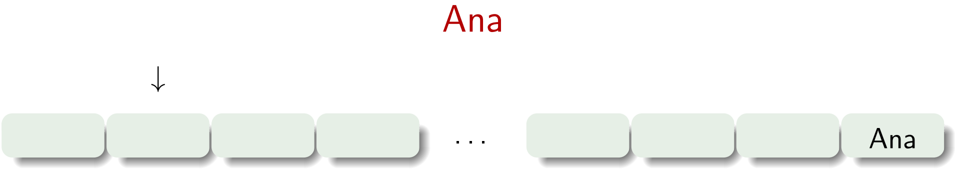
Ana



. . .

Ana

Busca linear



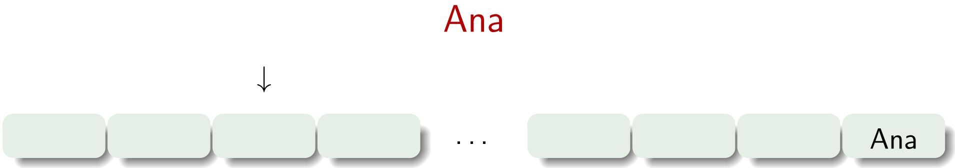
Ana

↓

. . .

Ana

Busca linear



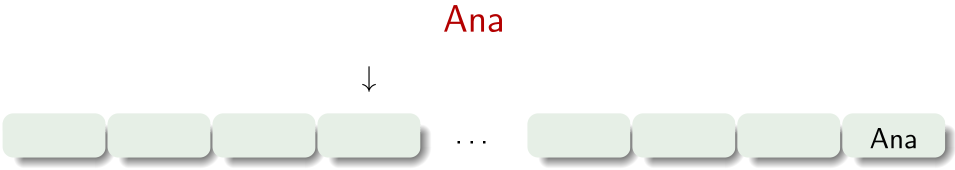
Ana

↓

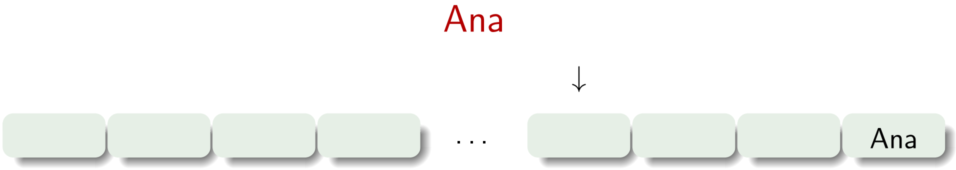
. . .

Ana

Busca linear



Busca linear



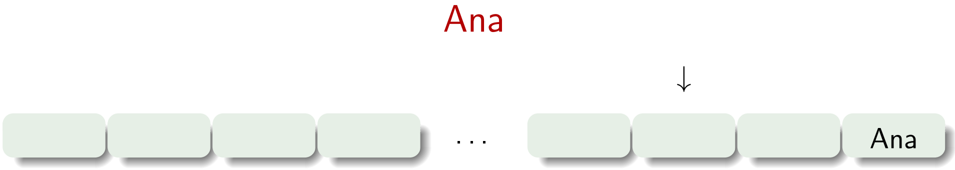
Ana

↓

. . .

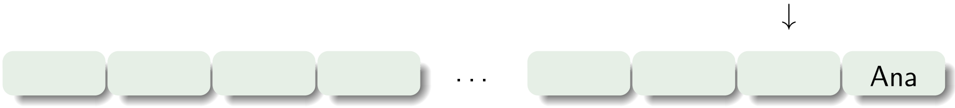
Ana

Busca linear



Busca linear

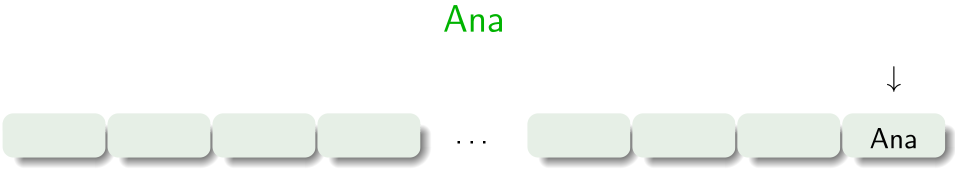
Ana



. . .

Ana

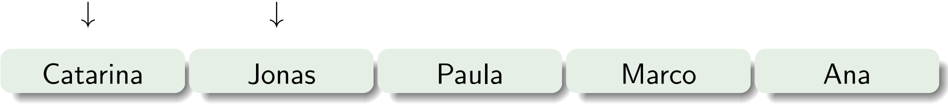
Busca linear



Busca linear

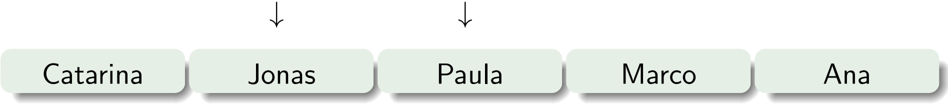
$$\approx x$$

Ordenação (Bubble sort)



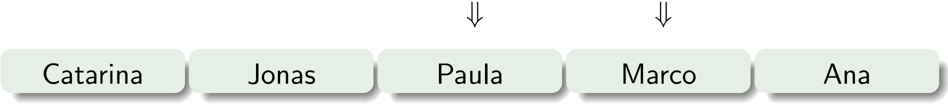
Catarina Jonas Paula Marco Ana

Ordenação (Bubble sort)



Catarina Jonas Paula Marco Ana

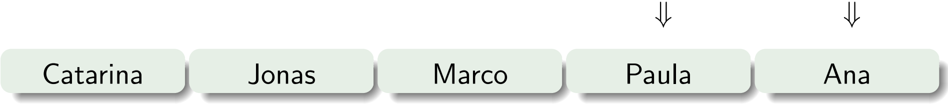
Ordenação (Bubble sort)



⇓ ⇓

Catarina Jonas Paula Marco Ana

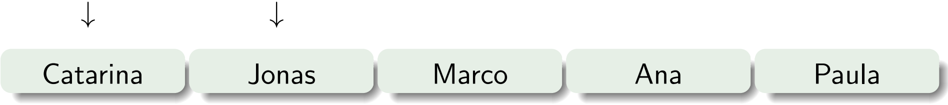
Ordenação (Bubble sort)



⇓ ⇓

Catarina | Jonas | Marco | Paula | Ana

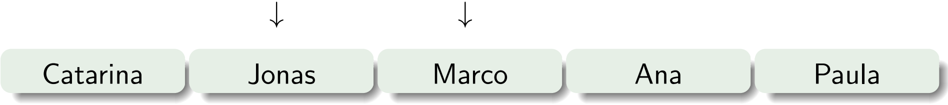
Ordenação (Bubble sort)



↓ ↓

Catarina Jonas Marco Ana Paula

Ordenação (Bubble sort)



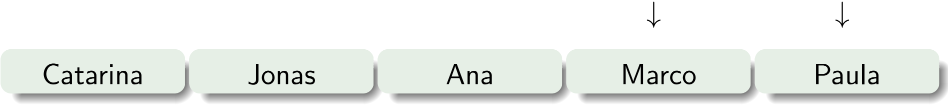
↓ ↓

Catarina Jonas Marco Ana Paula

Ordenação (Bubble sort)

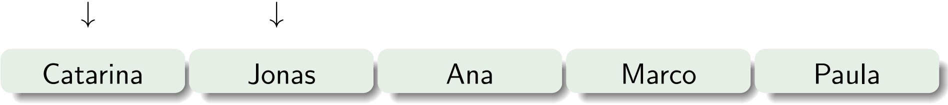
		⇓	⇓	
Catarina	Jonas	Marco	Ana	Paula

Ordenação (Bubble sort)



Catarina Jonas Ana Marco Paula

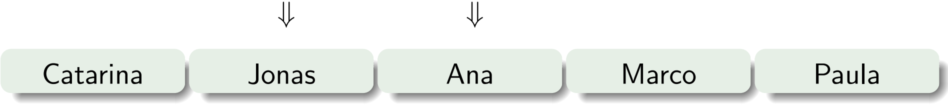
Ordenação (Bubble sort)



↓ ↓

Catarina Jonas Ana Marco Paula

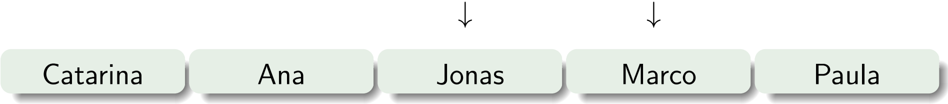
Ordenação (Bubble sort)



⇓ ⇓

Catarina | Jonas | Ana | Marco | Paula

Ordenação (Bubble sort)



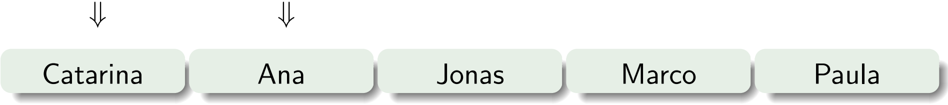
↓ ↓

Catarina | Ana | Jonas | Marco | Paula

Ordenação (Bubble sort)

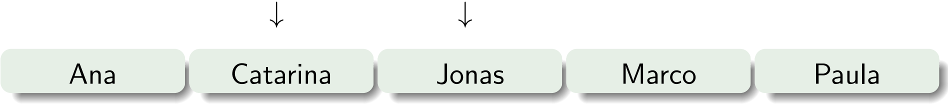
			↓	↓
Catarina	Ana	Jonas	Marco	Paula

Ordenação (Bubble sort)



⇓	⇓			
Catarina	Ana	Jonas	Marco	Paula

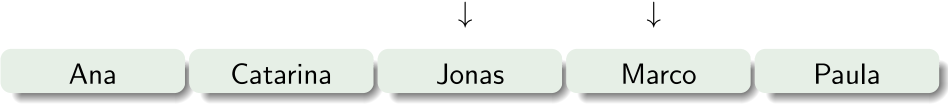
Ordenação (Bubble sort)



↓ ↓

Ana | Catarina | Jonas | Marco | Paula

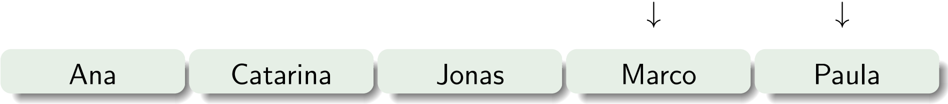
Ordenação (Bubble sort)



↓ ↓

Ana Catarina Jonas Marco Paula

Ordenação (Bubble sort)

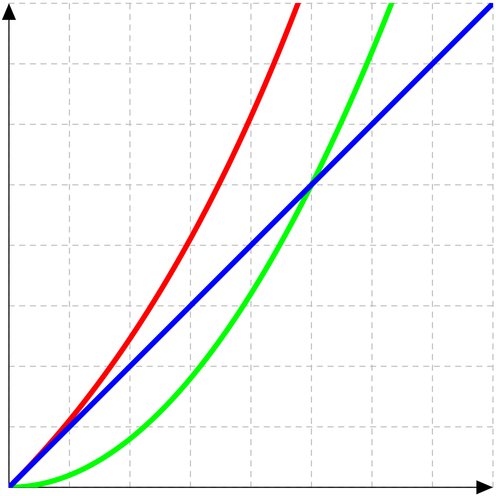


Ana Catarina Jonas Marco Paula

Ordenação (Bubble sort)

$$\approx x^2$$

Complexidade algorítmica

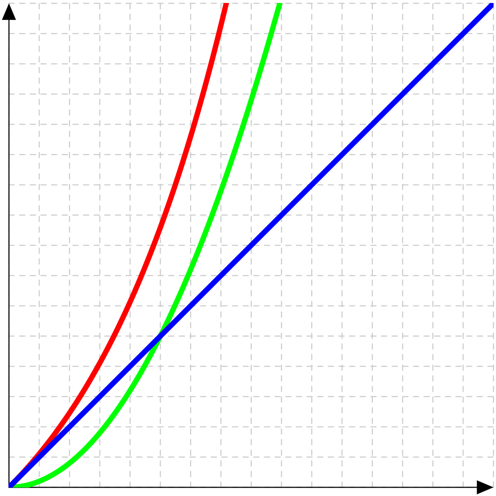


x

x^2

e^x

Complexidade algorítmica



x

x^2

e^x

Complexidade Algorítmica

$$X$$

Complexidade Algorítmica

$$x^2$$

Complexidade Algorítmica

$$x^{10}$$

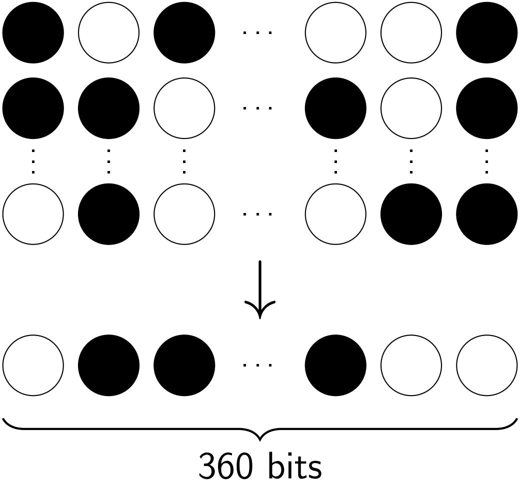
Complexidade Algorítmica

$$x^{7449279}$$

Complexidade Algorítmica

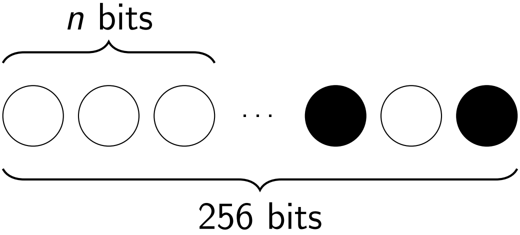
$$e^x$$

Pré-imagem de Hash



Pré-imagem de Hash

bitcoin



n bits

256 bits

Pré-imagem de Hash

$$\approx 2^{360}$$

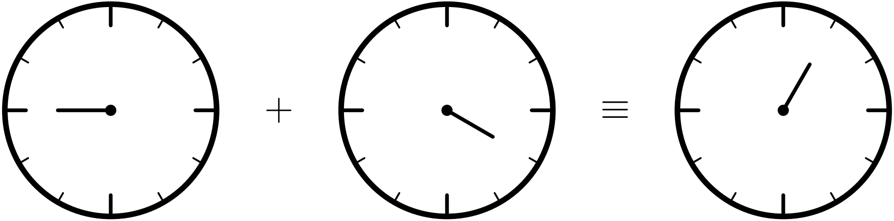
Pré-imagem de Hash

$$\underbrace{10^{80}}_{\text{Átomos no universo}} \times \underbrace{10^{10}}_{\text{10 GHz}} \times \underbrace{4,4 \cdot 10^{17}}_{\text{Idade do universo}}$$

$$\approx 2^{358}$$

P vs. NP

Aritmética módulo p



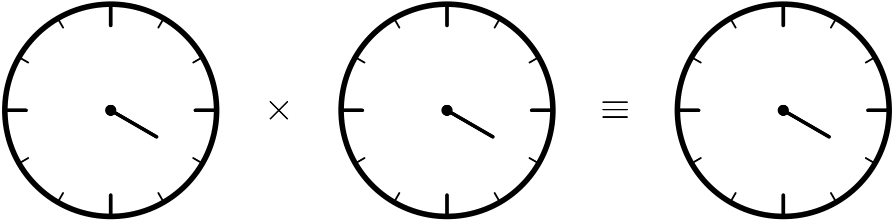
Aritmética módulo p

$$9 \quad + \quad 4 \quad \equiv \quad 13 \pmod{12}$$

Aritmética módulo p

$$9 \qquad + \qquad 4 \qquad \equiv \qquad 1 \pmod{12}$$

Aritmética módulo p



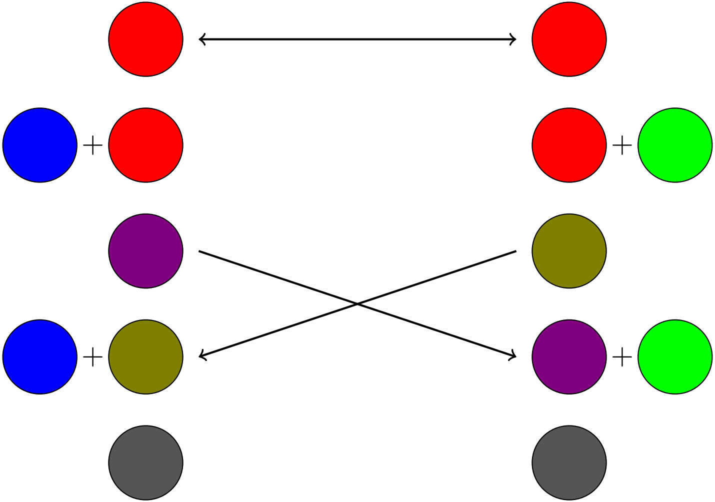
Aritmética módulo p

$$4 \quad \times \quad 4 \quad \equiv \quad 16 \pmod{12}$$

Aritmética módulo p

$$4 \quad \times \quad 4 \quad \equiv \quad 4 \pmod{12}$$

Diffie-Hellman



Diffie-Hellman

$$\begin{tikzcd}
p,\ g \arrow[r, leftrightarrow] & p,\ g \\
g^{a} \pmod{p} \arrow[dr] & g^{b} \pmod{p} \arrow[dl] \\
(g^{b})^{a} \pmod{p} & (g^{a})^{b} \pmod{p}
\end{tikzcd}$$

RSA

$$p, q$$

$$\vdots$$

$$n = pq$$

$$d = \cdots \qquad \longrightarrow \qquad n, e$$

$$e = \cdots$$

$$M^{de} \equiv M \text{ (mod n)}$$

RSA

$$\begin{tikzcd}
 & M^e \pmod{n} \arrow[dl] \\
(M^e)^d \pmod{n} &
\end{tikzcd}$$

Difícil?

Diffie-Hellman

Dados g, p e H, encontre a tal que $g^a \equiv H \pmod{p}$.

RSA

Dado n, encontre p e q tais que $n = pq$.

Difícil?

Logaritmo discreto

Dados g, p e H, encontre a tal que $g^a \equiv H \pmod{p}$.

Fatoração

Dado n, encontre p e q tais que $n = pq$.

Computação e criptografia quântica

Quebra DH, RSA, ECC...

Computação e criptografia quântica

Quebra DH, RSA, ECC...

Simétrica: BB84 + reconciliação + amplificação
Assimétrica e autenticação: Ring-LWE (NP-completo), NTRU

Computação e criptografia quântica

Quebra DH, RSA, ECC...

Simétrica: BB84 + reconciliação + amplificação
Assimétrica e autenticação: Ring-LWE (NP-completo), NTRU

Computação e criptografia quântica

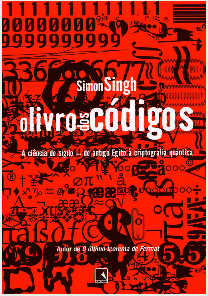
Quebra DH, RSA, ECC...

Simétrica: BB84 + reconciliação + amplificação
Assimétrica e autenticação: Ring-LWE (NP-completo), NTRU

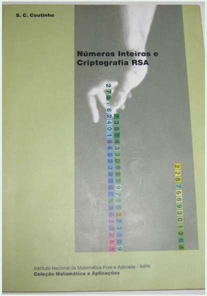
Supremacia quântica?

Apelo

Referências

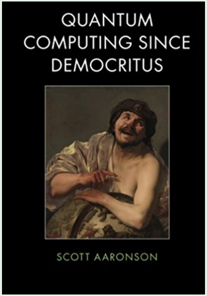

Simon Singh
o livro dos códigos
A ciência do sigilo – do antigo Egito à criptografia quântica
Autor de O último teorema de Fermat

O Livro dos Códigos
Simon Singh


S. C. Coutinho
Números Inteiros e Criptografia RSA
Instituto Nacional de Matemática Pura e Aplicada - IMPA
Coleção Matemática e Aplicações

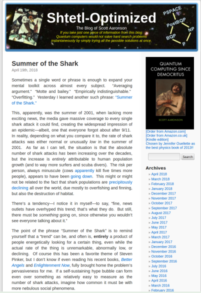
Números Inteiros e Criptografia RSA
Severino Collier Coutinho

Referências



Quantum Computing Since Democritus

Scott Aaronson



Shtetl-Optimized

The Blog of Scott Aaronson

If you take just one piece of information from this blog:
Quantum computers would not solve hard search problems
instantaneously by simply trying all the possible solutions at once.

Summer of the Shark

April 19th, 2018

Sometimes a single word or phrase is enough to expand your mental toolkit across almost every subject. "Averaging argument." "Motte and bailey." "Empirically indistinguishable." "Overfitting." Yesterday I learned another such phrase: "Summer of the Shark."

This, apparently, was the summer of 2001, when lacking more exciting news, the media gave massive coverage to every single shark attack it could find, creating the widespread impression of an epidemic—albeit, one that everyone forgot about after 9/11. In reality, depending on what you compare it to, the rate of shark attacks was either normal or unusually *low* in the summer of 2001. As far as I can tell, the situation is that the absolute number of shark attacks *has* been increasing over the decades, but the increase is *entirely* attributable to human population growth (and to way more surfers and scuba divers). The risk per person, always minuscule (cows apparently kill five times more people), appears to have been going down. This might or might not be related to the fact that shark populations are precipitously declining all over the world, due mostly to overfishing and finning, but also the destruction of habitat.

There's a tendency—I notice it in myself—to say, "fine, news outlets have overhyped this trend; that's what they do. But still, there must be *something* going on, since otherwise you wouldn't see everyone talking about it."

The point of the phrase "Summer of the Shark" is to remind yourself that a "trend" can be, and often is, **entirely** a product of people energetically looking for a certain thing, even while the actual rate of the thing is unremarkable, abnormally low, or declining. Of course this has been a favorite theme of Steven Pinker, but I don't know if even reading his recent books, *Better Angels* and *Enlightenment Now*, fully brought home the problem's pervasiveness for me. If a self-sustaining hype bubble can form even over something as relatively easy to measure as the number of shark attacks, imagine how common it must be with more nebulous social phenomena.

[Order from Amazon.com]
[Order from Amazon.co.uk]
[Kindle edition]
Chosen by Jennifer Ouellette as the best physics book of 2013!!

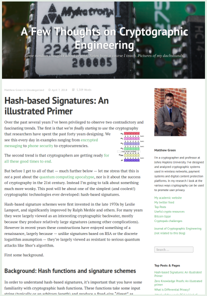
Archives

- April 2018
- March 2018
- February 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- July 2016
- June 2016
- May 2016
- April 2016
- March 2016
- February 2016

Shtetl-Optimized

Scott Aaronson

Referências



A Few Thoughts on Cryptographic Engineering

Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshunds.

Matthew Green in Uncategorized · April 7, 2018 · 5,309 Words

Hash-based Signatures: An illustrated Primer

Over the past several years I've been privileged to observe two contradictory and fascinating trends. The first is that we're *finally starting to use* the cryptography that researchers have spent the past forty years designing. We see this every day in examples ranging from encrypted messaging to phone security to cryptocurrencies.

The second trend is that cryptographers are getting ready for all these good times to end.

But before I get to all of that — much further below — let me stress that this is *not* a post about the quantum computing apocalypse, nor is it about the success of cryptography in the 21st century. Instead I'm going to talk about something much more wonky. This post will be about one of the simplest (and coolest!) cryptographic technologies ever developed: hash-based signatures.

Hash-based signature schemes were first invented in the late 1970s by Leslie Lamport, and significantly improved by Ralph Merkle and others. For many years they were largely viewed as an interesting cryptographic backwater, mostly because they produce relatively large signatures (among other complications). However in recent years these constructions have enjoyed something of a renaissance, largely because — unlike signatures based on RSA or the discrete logarithm assumption — they're largely viewed as resistant to serious quantum attacks like Shor's algorithm.

First some background.

Background: Hash functions and signature schemes

In order to understand hash-based signatures, it's important that you have some familiarity with cryptographic hash functions. These functions take some input string (typically or an arbitrary length) and produce a fixed-size "digest" as

Matthew Green

I'm a cryptographer and professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used to promote user privacy.

My academic website
My twitter feed
Top Posts
Useful crypto resources
Bitcoin tipjar
Cryptopals challenges

Journal of Cryptographic Engineering (not related to this blog)

Search ...

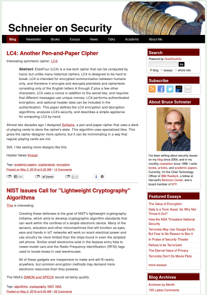
Top Posts & Pages

Hash-based Signatures: An Illustrated Primer
Zero Knowledge Proofs: An illustrated primer
What is Differential Privacy?

A Few Thoughts on Cryptographic Engineering

Matthew Green

Referências



Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic | About Me

LC4: Another Pen-and-Paper Cipher

Interesting symmetric cipher: LC4:

> **Abstract:** ElsieFour (LC4) is a low-tech cipher that can be computed by hand; but unlike many historical ciphers, LC4 is designed to be hard to break. LC4 is intended for encrypted communication between humans only, and therefore it encrypts and decrypts plaintexts and ciphertexts consisting only of the English letters A through Z plus a few other characters. LC4 uses a nonce in addition to the secret key, and requires that different messages use unique nonces. LC4 performs authenticated encryption, and optional header data can be included in the authentication. This paper defines the LC4 encryption and decryption algorithms, analyzes LC4's security, and describes a simple appliance for computing LC4 by hand.

Almost two decades ago I designed Solitaire, a pen-and-paper cipher that uses a deck of playing cards to store the cipher's state. This algorithm uses specialized tiles. This gives the cipher designer more options, but it can be incriminating in a way that regular playing cards are not.

Still, I like seeing more designs like this.

Hacker News thread.

Tags: academic papers, cryptanalysis, encryption
Posted on May 3, 2018 at 6:42 AM • 14 Comments

NIST Issues Call for "Lightweight Cryptography" Algorithms

This is interesting:

> Creating these defenses is the goal of NIST's lightweight cryptography initiative, which aims to develop cryptographic algorithm standards that can work within the confines of a simple electronic device. Many of the sensors, actuators and other micromachines that will function as eyes, ears and hands in IoT networks will work on scant electrical power and use circuitry far more limited than the chips found in even the simplest cell phone. Similar small electronics exist in the keyless entry fobs to newer-model cars and the Radio Frequency Identification (RFID) tags used to locate boxes in vast warehouses.
>
> All of these gadgets are inexpensive to make and will fit nearly anywhere, but common encryption methods may demand more electronic resources than they possess.

The NSA's SIMON and SPECK would certainly qualify.

Tags: algorithms, cryptography, NIST, NSA
Posted on May 2, 2018 at 6:40 AM • 29 Comments

Search

Powered by DuckDuckGo

● blog ○ essays ○ whole site

Subscribe

About Bruce Schneier

I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of EFF.

Featured Essays

- The Value of Encryption
- Data Is a Toxic Asset, So Why Not Throw It Out?
- How the NSA Threatens National Security
- Terrorists May Use Google Earth, But Fear Is No Reason to Ban It
- In Praise of Security Theater
- Refuse to be Terrorized
- The Eternal Value of Privacy
- Terrorists Don't Do Movie Plots

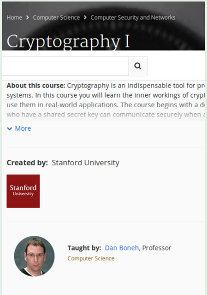
more essays

Blog Archives

- Archives by Month
- 100 Latest Comments

Schneier on Security

Bruce Schneier



Home › Computer Science › Computer Security and Networks

Cryptography I

About this course: Cryptography is an indispensable tool for pr
systems. In this course you will learn the inner workings of crypt
use them in real-world applications. The course begins with a d
who have a shared secret key can communicate securely when a

⌄ More

Created by: Stanford University

Taught by: Dan Boneh, Professor
Computer Science

Cryptography I

Dan Boneh

Referências

UDACITY

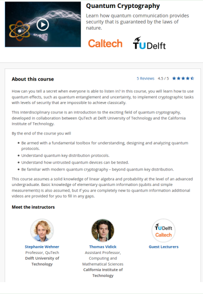
Applied Cryptography

Science of Secrets

START FREE COURSE

Applied Cryptography

Dave Evans



Quantum Cryptography

Learn how quantum communication provides security that is guaranteed by the laws of nature.

Caltech TUDelft

About this course

5 Reviews 4.5 / 5 ★★★★☆

How can you tell a secret when everyone is able to listen in? In this course, you will learn how to use quantum effects, such as quantum entanglement and uncertainty, to implement cryptographic tasks with levels of security that are impossible to achieve classically.

This interdisciplinary course is an introduction to the exciting field of quantum cryptography, developed in collaboration between QuTech at Delft University of Technology and the California Institute of Technology.

By the end of the course you will

- Be armed with a fundamental toolbox for understanding, designing and analyzing quantum protocols.
- Understand quantum key distribution protocols.
- Understand how untrusted quantum devices can be tested.
- Be familiar with modern quantum cryptography – beyond quantum key distribution.

This course assumes a solid knowledge of linear algebra and probability at the level of an advanced undergraduate. Basic knowledge of elementary quantum information (qubits and simple measurements) is also assumed, but if you are completely new to quantum information additional videos are provided for you to fill in any gaps.

Meet the instructors

Stephanie Wehner
Professor, QuTech
Delft University of Technology

Thomas Vidick
Assistant Professor, Computing and Mathematical Sciences
California Institute of Technology

Guest Lecturers

Quantum Cryptography

Stephanie Wehner e *Thomas Vidick*

Referências

Sites:

https://www.scottaaronson.com/blog/

https://blog.cryptographyengineering.com/

https://www.schneier.com/

https://www.coursera.org/learn/crypto

https://udacity.com/course/applied-cryptography--cs387

https:
//www.edx.org/course/quantum-cryptography-caltechx-delftx-qucryptox-0

Referências

Imagens:

https://www.vectorportal.com/stockvectors/Technology/desktop-personal-computer-vector/12976.aspx

https://bitcoin.org/img/icons/logotop.svg

https://images-na.ssl-images-amazon.com/images/I/819HiREnxsL.jpg

https://www.publicdomainpictures.net/view-image.php?image=76327