Criptologia Aplicada

Quebra de Senhas

Dênio Mariz
denio@ifpb.edu.br

Quão forte é uma senha?

- Uma senha é tão forte quanto o número de combinações possíveis de se formar, considerando:
  - Conjunto de caracteres usado
  - Tamanho da senha
- $F = |C|^N$
  - F = número de combinações
  - $|C|$ = tamanho do conjunto C de caracteres
  - N = tamanho da senha

O impacto do tamanho da chave

Tamanho da Chave	Possibilidades	Computador 1 10^6/s
32 bits	$2^{32}=4.2x10^9$	71 minutos
56 bits	$2^{56}=7.2x10^{16}$	2285 anos

Chave maior reduz impacto do poder computacional

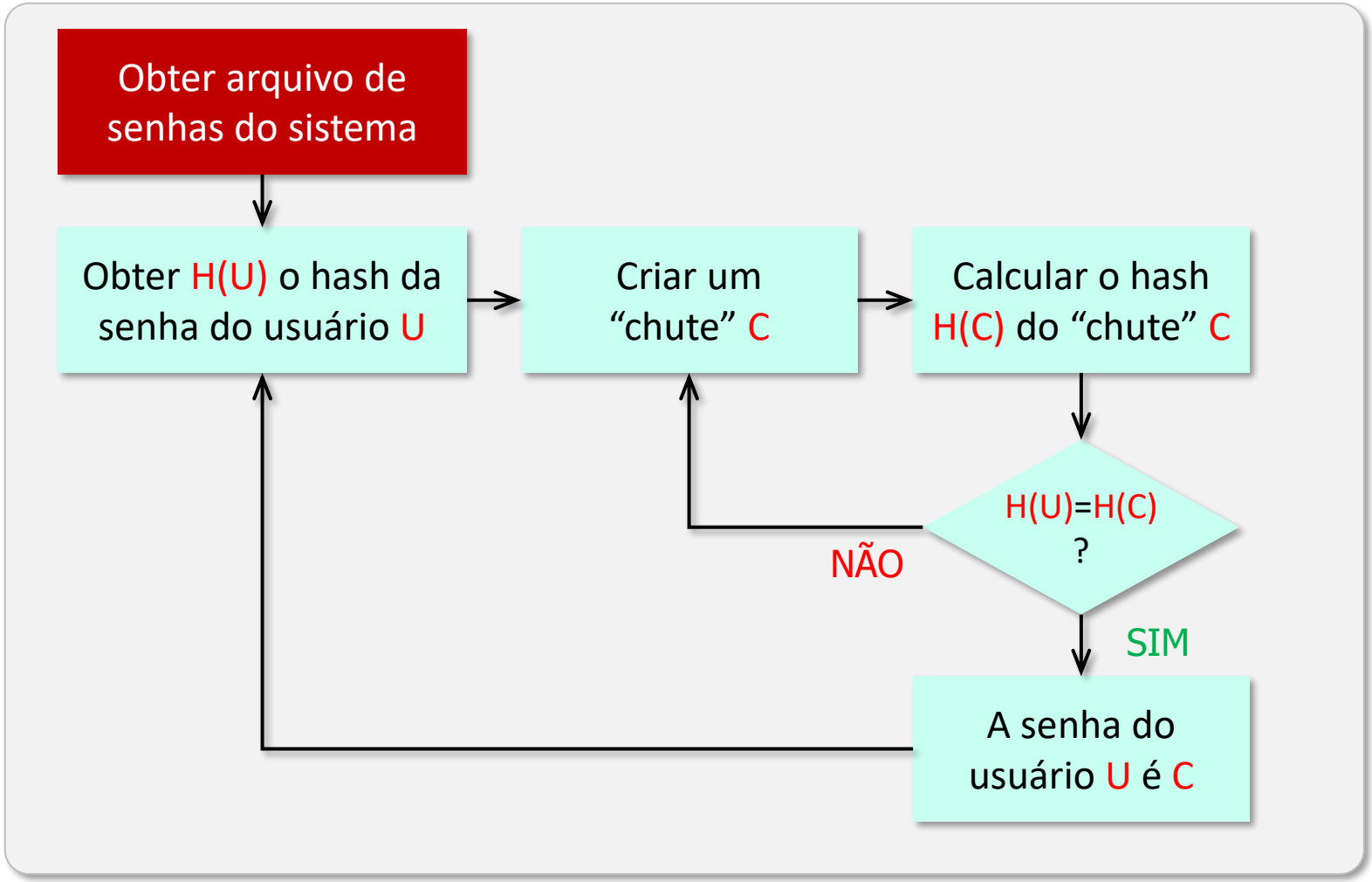
Computador
1 milhão de vezes mais rápido

Para dar ideia de grandeza de $\mathbf{2^{128}}$:
Idade do universo = 13.8 Bilhões de anos < de 2^{69} milisegundos

Motivação para "password cracking"

- Ponto de vista do Invasor
  - Precisa de um login para escalar privilégios – tentam adivinhar senhas "fracas"
  - Roubam arquivos de senhas em sistemas fracos e tentam as senhas dos mesmos usuários em outros sistemas
    - **Usuários usam senhas iguais em sistemas diferentes**
    - **Algumas senhas usadas durante anos, alternadamente**
    - **Sua senha do login = senha de banco ? se for, "tchau!"**
- Ponto de vista do Administrador
  - "A corrente é tão forte quanto seu elo mais fraco"
  - precisam saber se as senhas dos usuários são "fracas"
  - Como? Tentando quebrar!
  - Avisando usuários de senha fraca para trocá-las
  - Administrador não precisa ver a senha

Algoritmo “Força Bruta”



Tipos de "chute"

- Baseado em dicionários
  - Todas as palavras do dicionário + Gírias + etc …
  - Dicionário fica em um arquivo
- Dicionário combinado
  - Chutes com prefixo e sufixo
  - Exemplo: login ana, chutes: 1ana, 123ana, ana1, ana123, …
- "Força bruta"
  - Tenta todas as possíveis combinações de caracteres
  - a-z, A-Z, 0-9, !@#$%^&*()_+=-~?<>"':;][{}\|
  - Tempo de quebra depende o tamanho da senha
  - Conclusão: senhas maiores são mais difíceis de advinhar

Passwords mais usadas (2008)

- 123456
- password
- 12345678
- 1234
- pussy
- 12345
- dragon
- qwerty
- 696969
- mustang
- letmein
- baseball
- master
- michael
- football
- shadow
- monkey
- abc123
- pass
- fuckme
- 6969
- jordan
- harley
- ranger
- iwantu
- jennifer
- hunter
- fuck
- 2000
- test
- batman
- trustno1
- thomas
- tigger
- robert
- access
- love
- buster
- 1234567
- soccer
- hockey
- killer
- george
- sexy
- andrew
- charlie
- superman
- asshole
- fuckyou
- dallas

http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

Passwords mais usadas (2014)

- 123456
- password
- 12345678
- qwerty
- abc123
- 123456789
- 111111
- 1234567
- iloveyou
- adobe123
- 123123
- Admin
- 1234567890
- letmein
- photoshop
- 1234
- monkey
- shadow
- sunshine
- 12345
- password1
- princess
- azerty
- trustno1
- 000000

http://gizmodo.com/the-25-most-popular-passwords-of-2013-god-help-us-1504852434

Sua senha é boa?

- http://www.passwordmeter.com
- https://howsecureismypassword.net
- https:http://www.trypap.com