DWD12 – Um Método para criação de senhas seguras e memorizáveis

Cárlisson Galdino

Rômulo Nunes Oliveira

Raiela Quirino Lima

O Problema das Senhas

Senhas Fáceis

Padrões fáceis (“12345”, “qwerty”...)

Alterados (“m@ria”, “g4rfi3ld”)

Senhas Difíceis

Aleatório (“~MS{dg[d”, “wiv3h7rw”)

Ataque de dicionário

Automação das checagens

Passphrases

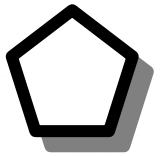
A multiplicação das palavras

SECURITY

No password is safe from this new 25-GPU computer cluster

The setup uses 25 AMD Radeon graphics cards and can make 350 billion guesses per second. All eight-character passwords fall in hours; some take only six minutes.

BY DON REISINGER | DECEMBER 10, 2012 9:35 AM PST



DWD12

Diceware

Aleatoriedade real

A Entropia de uma frase aleatória

1 palavra = 7.776 possibilidades = 12,9 bits de entropia

Tão seguro quanto uma senha de 2 caracteres alfanuméricos

6 palavras = $2{,}2 * 10^{23}$ possibilidades = 77,5 bits de entropia

Tão seguro quanto uma senha de 13 caracteres alfanuméricos

O que é mais fácil de lembrar?

Cacho noção clareza dario longo emirado

txGxq8HPC3spN

Quando entra no email
Já aparece pra mudar
Ele resolve apertar
Num botão ali no meio
"Gera senha", sem rodeio
Gera uma senha segura
Ele fala: "que loucura!
Senha doida pra danar!
Como é que vou lembrar?
Senha grande e obscura!"

É verdade, a senha tinha
Letra, número e arroba
"Senha difícil da boba!
Mas não vou fazer gracinha
Essa senha vai ser minha
Pra proteger meu email
Duvido que alguém hackeie
Ene xis bê sublinhado
O xis e o bê aumentados
Arroba três efe seis

DWD12

Diceware D12

- Dados de 12 lados
  - Adaptável para outras formas, como dados comuns e moedas
- Uso de tomos
- Uso de um tomo secreto
- Tomos como listagens temáticas
- Rolagens com significado

Comparando Diceware com DWD12

	Diceware	1 tomo	4 tomos	6 tomos	12 tomos
Tipo de dado	d6	d12	d12	d12	d12
Rolagens de dados	5	3	4	4	4
Palavras possíveis	7.776	1.728	6.912	10.368	20.736
Entropia aproximada	12,92	10,75	12,75	13,34	14,34
Senha de 64 bits	5	6	5	5	5
Senha de 128 bits	10	12	10	10	9

Diceware D12 Hoje

Regras definidas

Método alternativo em estudo

- Senha curtas

Conjunto Inicial

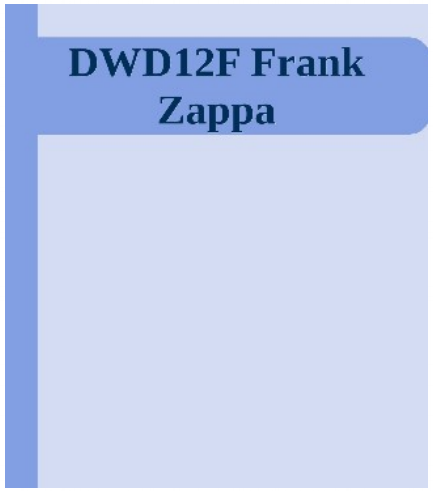
- Palavras em Português
- 12 tomos de palavras comuns (escritores, compositores, estados brasileiros...)
- 4 tomos especiais
- Diagramados principalmente para impressão em folhetos A6

Conjunto Fast

- Palavras em Inglês
- 6 tomos de palavras comuns (compositores)
- Diagramados principalmente como ebook ePub

Tomos Públicos Comuns

Tomo	Conjunto	Idioma	Tamanho méd
Diceware Castelo Branco - Em PDF	Inicial	Português	6,93
Diceware Chico - Em PDF	Inicial	Português	8,67
Diceware Eliana - Em PDF	Inicial	Português	8,45
Diceware Elton John - Em PDF	Fast	English	7,93
Diceware Elvis Presley - Em PDF	Fast	English	7,46
Diceware Estados - Em PDF	Inicial	Português	9,50
Diceware Frank Sinatra - Em PDF	Fast	English	6,59
Diceware Frank Zappa - Em PDF	Fast	English	7,67
Diceware George Jones - Em PDF	Fast	English	7,15



Próximos Passos

Projeto de software

- Scripts de geração de tomos e validação
- Scripts de geração de senhas
- Bibliotecas para geração de senhas (inserível em softwares da instituição)

Continuação do conjunto Fast

Divulgação do DWD12 na cidade e entre a comunidade acadêmica

Agradecimentos

Perguntas

wiki.cordeis.com

Local provisório

DWD12 é um jeito
Dos melhores que se tenha
De se gerar uma senha
Segura mas com efeito
Que não a esquece o sujeito
Usando um dado que nem
De RPG pra ninguém
Descobrir, vá lá meu bom
wiki em cordeis.com
Crie sua senha também