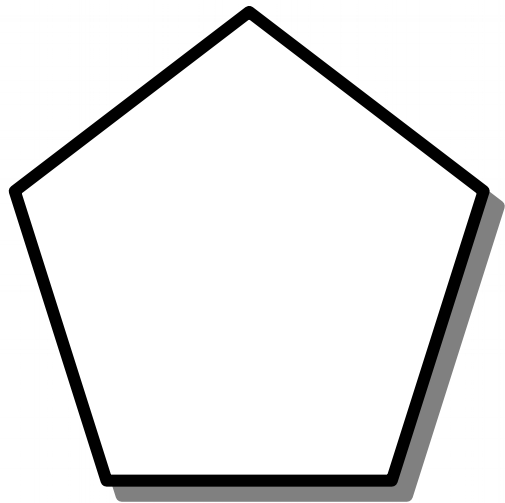
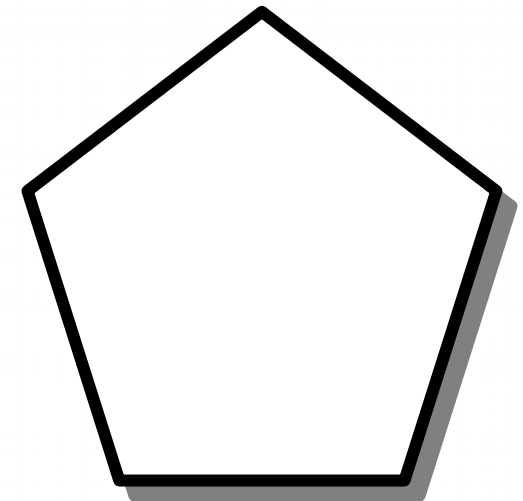


DWD12 – Um Método para criação de senhas seguras e memorizáveis



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

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*



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

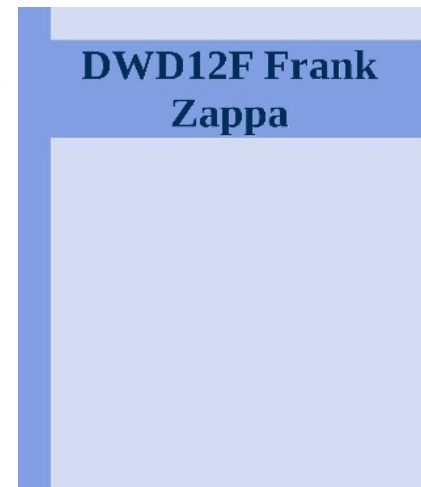
Palavras em Inglês

6 tomos de palavras comuns (compositores)

Diagramados principalmente como ebook ePub

Tomos Públicos Comuns

Tomo	Conjunto	Idioma	Tamanho mé
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



Diceware D12 Castelo Branco 3/12

1. vexo 2. tímido 3. zelei 4. adiar 5. amo-o 6. armem 7. barda 8. bardo 9. crivo 10. de-lu 11. de-põe 12. doira	1. esgar 2. expia 3. firas 4. flur 5. fumos 6. galta 7. galãs 8. lardo 9. lerei 10. lidei 11. lidou 12. odiei	1. pence 2. pomos 3. pruir 4. reajo 5. relei 6. remiu 7. sujam 8. urdem 9. doe-me 10. lexis 11. ordenam 12. parras	1. riu-se 2. rolica 3. tojal 4. adorou 5. adoçou 6. alizer 7. ajudei 8. alardo 9. alisou 10. ari-me 11. animam 12. apoiou
1. assise 2. aterre 3. azados 4. azardo 5. azares 6. aziaga 7. beirão 8. brinde 9. briosa 10. calçam 11. candor 12. captar	1. carpia 2. cessem 3. chorem 4. churma 5. coaram 6. cobreí 7. coburo 8. crepes 9. decoro 10. delido 11. deliro 12. elegeu	1. enlevo 2. espias 3. espriu 4. estifo 5. expire 6. faceta 7. fardes 8. farija 9. fausta 10. febre 11. fechem 12. firmas	1. fiz-me 2. forçou 3. gordes 4. gúido 5. herdar 6. instar 7. instou 8. jantei 9. jocosso 10. lateje 11. lautos 12. liames
1. limpei 2. liras 3. loiros 4. lucida 5. miadres 6. mata-o 7. matado 8. meigos 9. mentor 10. mistos 11. mofina 12. mortas	1. motejo 2. murças 3. nediez 4. nevoas 5. nivela 6. nomear 7. nomeia 8. noutes 9. noviço 10. obvio 11. obviou 12. odiada	1. oleosa 2. osculo 3. palcos 4. palhas 5. pascia 6. passas 7. pautou 8. pegões 9. possas 10. preto 11. prive 12. pungia	1. pungr 2. quave 3. radlar 4. rangir 5. rapto 6. raspou 7. reagia 8. reagir 9. releva 10. renove 11. reveza 12. sanear



Próximos Passos

Projeto de software

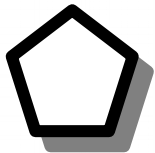
Scripts de geração de tomos e validação

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



DWD12

Momentos Finais

Agradecimentos

Perguntas

wiki.cordeis.com

Local provisório



**KIT
SEGURANÇA**

**MÉTODO PARA CRIAÇÃO
DE SENHAS SEGURAS
E FÁCEIS DE LEMBRAR**

**DWD12 + 13 CORDÉIS!
+ DADO**

*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*