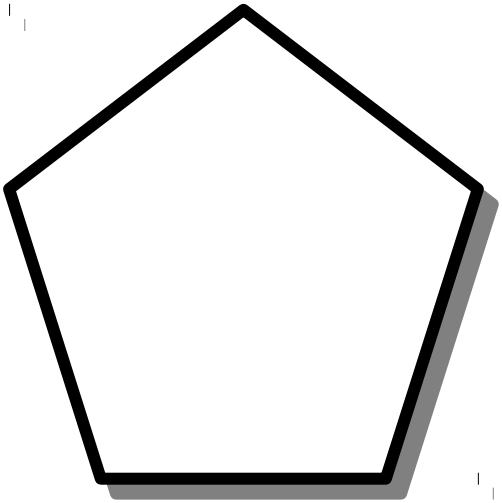

Diceware D12
Regras Gerais

Diceware D12

Diceware é um método de criação de senhas elaborado por Arnold Reinhold e publicado em 1995. Nesse método, você sorteia algumas palavras (geralmente entre 4 e 8 palavras) a partir de uma lista enorme (uma lista de 7.776 palavras para ser exato) utilizando dados comuns, de seis faces, e esta é sua senha. Mesmo a lista total sendo pública, a chance de ser quebrada é pequena, pois é de 1 em x^y, sendo x o total de palavras da lista e y o número de sorteios. A chance de adivinhar uma senha de 5 palavras em uma tentativa, por exemplo, é de 1 em 7.776^5, o que dá 1 em 28.430.288.029.929.701.376! Ou aproximadamente 1 em 2,8 * 10^{19}! Cada palavra é sorteada a partir de 5 rolagens de dados. Você pode entender melhor a proposta lendo o artigo de Micah Lee para The Intercept, entitulado Senhas fáceis para você memorizar e que nem a NSA conseguirá desvendar.

A proposta Diceware D12 (ou DW12) é de uma variante do Diceware tradicional, com algumas diferenças marcantes:

- Uso de dados de 12 faces. Dados de 12 faces oferecem individualmente um número bom de possibilidades. Podem ser substituídos por 2 rolagens de um dado de 6 faces ou mesmo por um baralho após uma adaptação rápida. Embora incomuns, estão presentes em qualquer “conjunto de dados para RPG”.
- Ao invés de uma lista única de palavras, o DW12 utiliza o conceito de tomos. Antes de sortear, você escolhe tomos de onde será feito o sorteio. Cada tomo contém 1.728 palavras, de modo que o uso de 5 tomos já supera o Diceware tradicional em entropia (totaliza 8.640 palavras). Sem contar que para tentar quebrar sua senha, mesmo que o atacante conheça o método DW12, ele não saberá que subconjunto de tomos você utilizou. E a senha se torna ainda mais difícil se utilizamos um “tomo secreto”.

Cada tomo DW12 é composto por 12 páginas; cada página tem 12 sessões e cada sessão tem 12 palavras. Assim, você sorteia a palavra em um tomo a partir de 3 rolagens de dados (ou 6, se forem dados de 6 faces). Feita esta introdução, vamos às sessões deste wiki para dúvidas, questões e recursos mais específicos:

Diceware e Diceware D12

Critério	Diceware	DWD12 c/4 tomos	DWD12 c/5 tomos	DWD12 c/6 tomos	DWD12 c/12 tomos
Tipo de dado	6 faces	12 faces	12 faces	12 faces	12 faces
Quantidade de rolagens	5	4	4	4	4
Total de palavras	7776	6912	8640	10368	20736
Entropia	~12.92	~12.75	~13.07	~13.34	~14.34

Escolhendo os Tomos

Como o método DWD12 é baseado em tomos, você precisa escolher primeiro que tomos utilizará. Pode utilizar apenas 1 tomo, mas aí sua senha pode não ficar tão segura no final. Você deve juntar ao menos 4 tomos. Idealmente, seriam 6 tomos, sendo 1 deles secreto. É complicado e trabalhoso fazer um tomo secreto, então talvez só seja viável se for compartilhado por um grupo (funcionários de uma empresa, colegas de turma de uma universidade, ou até grupos maiores).

Este wiki oferecerá alguns tomos para sua escolha. Uma vez definidos que tomos você vai utilizar, coloque-os numa sequência. Para cada palavra que for sortear, antes de sortear a palavra, você sorteará um tomo. Isso pode ser feito com o dado de 12 faces, independente de quantos tomos você use:

Rolagem de Escolha do Tomo

Escolhido	2 tomos	3t	4t	5t	6t	7t	8t	9t	10t	11t	12 tomos
Jogue de novo	-	-	-	11-12	-	8-12	9-12	10-12	11-12	12	-
Escolha o 1º tomo	1-6	1-4	1-3	1-2	1-2	1	1	1	1	1	1
Segundo tomo	7-12	5-8	4-6	3-4	3-4	2	2	2	2	2	2
Terceiro tomo	-	9-12	7-9	5-6	5-6	3	3	3	3	3	3
Quarto tomo	-	-	10-12	7-8	7-8	4	4	4	4	4	4
Quinto tomo	-	-	-	9-10	9-10	5	5	5	5	5	5
Sexto tomo	-	-	-	-	11-12	6	6	6	6	6	6
Sétimo tomo	-	-	-	-	-	7	7	7	7	7	7
Oitavo tomo	-	-	-	-	-	-	8	8	8	8	8
Nono tomo	-	-	-	-	-	-	-	9	9	9	9
Décimo tomo	-	-	-	-	-	-	-	-	10	10	10
Décimo primeiro	-	-	-	-	-	-	-	-	-	11	11
Décimo segundo	-	-	-	-	-	-	-	-	-	-	12

O Tamanho da Frase

Diceware tradicional recomenda senhas compostas por 6 palavras. Isso dá 77,52 bits de entropia. Usando DWD12 com 4 tomos, a qualidade da senha será pouco inferior à do Diceware tradicional: 76,5. A recomendação tende a continuar sendo a de fazer senha com 6 palavras, pois nem mesmo utilizando 12 tomos você consegue com 5 palavras atingir o nível de segurança do Diceware tradicional com 6 palavras (5 palavras em 12 tomos dá 71,7 bits de entropia).

Claro que as peculiaridades do DWD12 incluem a recomendação de manter um tomo secreto e a possibilidade de existirem em algum momento muitos tomos. Então na prática, mesmo que a segurança medida em bits de entropia seja equiparada, na prática a segurança do DWD12 tende a ser maior (caso as recomendações sejam seguidas). Mesmo porque essa medida (bits de entropia) leva em conta que o atacante conhece a lista de palavras que você utilizou para gerar a senha e que as palavras estão tal qual estão!

O Tamanho da Frase

Você pode reduzir o número de palavras que compoem sua senha se aplicar algumas transformações nas palavras usadas (seguindo as instruções da sessão “Método alternativo”). Por exemplo: se você usar apenas 4 tomos e sortear apenas 4 palavras, desde que em uma delas aplique 3 transformações e aplique apenas 1 transformação em outra (deixando as outras duas tal qual estavam, já conseguirá um grau de entropia maior: 79,66 bits! Claro, considerando-se que as transformações sejam objetivas, o que também não é o caso para todas elas (e na prática o nível de segurança seria ainda maior).

Resumindo, é isso:

- Pra ser tradicional, 6 palavras
- Pra ser “compacto”, 4 palavras, mas aplicando o “método alternativo” em uma delas (3x) e apenas uma transformação em outra
- Se chegarmos a ter 12 tomos: 4 palavras, aplicando o “método alternativo” a uma delas

Claro, nada te impede de criar senhas maiores ou menores conforme a necessidade/vontade… (o que provável e inevitavelmente aumentará ou diminuirá a segurança)

Tomos Secretos

Um tomo secreto nada mais é do que um tomo (com suas 12 páginas de 12 sessões de 12 palavras) com conteúdo preferencialmente inédito em relação aos demais tomos (como qualquer tomo novo), mas que não é publicado. Essa “garantia” de que o atacante não conhece o tomo aumenta ainda mais a segurança da senha. Se você usar 1 tomo secreto e 3 públicos, caso o atacante tenha acesso ao tomo secreto, a senha ainda será tão segura quanto uma gerada por 4 tomos públicos. Ou seja, a segurança da senha não depende de o tomo ser verdadeiramente secreto, mas aumenta caso ele continue sendo.

Para fazer um tomo novo, você deve ir colocando as palavras em um editor de textos, organizando nas divisões do DWD12 (agrupamentos de 12). É desejável que você, para cada palavra nova, cheque se ela já foi utilizada. A forma mais simples que vejo de fazer isso é criando um outro documento onde você colará todas as palavras de tomos que estão neste wiki (sim, criando um arquivo único, blocão, txt). Assim, ao escolher uma nova palavra, antes de escrevê-la no arquivo do seu tomo, você busca se ela existe nesse arquivo do blocão.

Uma vez tendo o tomo secreto, você tem basicamente 2 formas de utilizá-lo: tratando-o como público (para efeitos de geração de senha) ou garantindo que uma palavra vem dele.

Tratando como Público

Não há muito o que fazer. Ao colocar os tomos (escolhendo qual é o 1, qual o 2, etc), você simplesmente coloca o tomo secreto no meio deles e segue o procedimento normal.

Garantindo o Tomo Secreto

Neste caso,você faz o seguinte:

1) Escolha a quantidade de palavras que a senha terá
2) Jogue um dado para sortear uma posição (por exemplo: escolhi que terá 6 palavras, então jogo 1d12 e divido por 2 arredondando pra cima. Se sair 7, significa que a posição escolhida foi a 4ª)
3) Sorteie uma palavra do tomo secreto e a coloque na posição escolhida no passo anterior
4) Com o restante das palavras, siga o procedimento de sorteio normal

Para quem não tem um D12

O dado de 12 faces, base para o DWD12, pode ser encontrado em lojas de RPG, tanto lojas físicas quano virtuais. Em lojas físicas tende a ser mais fácil comprar apenas os dados de 12 faces. É bem possível que você precise comprar um conjunto de dados, que inclui um dado de 4 faces, um de 6, um de 8, um de 10, um de 20 e, finalmente, o de 12 faces.

Mas enquanto a encomenda de dados não chega (ou caso você simplesmente não queira comprar esse dado exótico), você pode gerar números aleatórios no intervalo de 1 a 12 de outras formas.

Usando Dados Comuns

O primeiro instinto ao tentar usar dados comuns é rolar dois dados e somar, mas isso não funciona. Primeiro, porque você nunca tirará “1”. Segundo porque a chance de cada número no espectro 2-12 será distinta. A chance de tirar 2 é de 1 em 36 enquanto a chance de tirar 7 é de 1 em 6! Então é sim possível (e fácil) usar dois dados de 6 para substituir o de 12 faces, mas o caminho é outro.

Você rolará um dado por vez ou rolará dados de cores ou aspectos diferentes, escolhendo um para ser o delimitador e outro para ser o definidor. O dado delimitador dirá qual o intervalo que outro dado vai cobrir. Se você tirar 1-3 no delimitador, o definidor agirá no intervalo 1-6; se sair 4-6, o definidor agirá no intervalo 7-12. Desse jeito, você sorteia exatamente no intervalo 1-12 e ao mesmo tempo mantém a mesma chance de resultado para cada um dos 12 números.

Se achou isso tudo confuso, sem problema! Basta usar a tabela abaixo!

Dado Delimitador	1 2 3	1 2 3	1 2 3	1 2 3	1 2 3	1 2 3	4 5 6	4 5 6	4 5 6	4 5 6	4 5 6	4 5 6
Dado Definidor	1	2	3	4	5	6	1	2	3	4	5	6
Resultado	1	2	3	4	5	6	7	8	9	10	11	12

Usando Cartas

Outra forma de substituir o dado de 12 faces é utilizando um baralho normal. Para torná-lo um substituto melhor, retire do baralho os coringas e reis. Se preferir, você pode deixar o baralho completo e simplesmente ignorar o resultado sempre que sair um rei ou coringa.

Lembre-se porém que, diferente do que ocorre com dados, o baralho é um sorteio sem reposição. Isso significa que ao tirar, por exemplo, um 3 de copas, a chance de tirar outro 3 será menor que a de tirar um 4. Por isso, é recomendável que, a cada carta tirada, devolva a carta ao baralho e reembaralhe.

Veja a tabela de decaimento de chances, dependendo também do número de maços que compoem o seu baralho. Para isso, consideramos que reis e coringas já foram exluídos. Lembrando que cada maço contém 4 cartas de cada número (uma por naipe).

Nº de maços	1D12	Baralho cheio	Chance de repetir o número	Chance de 2ª repetição	3ª repetição
1	8,3%	8,3%	6,2%	4,1%	2,1%
2	8,3%	8,3%	7,3%	6,2%	5,2%
3	8,3%	8,3%	7,6%	6,9%	6,2%
4	8,3%	8,3%	7,8%	7,3%	6,7%

Usando Cartas

Sugestão: se quiser mesmo reaproveitar o baralho para tirar mais resultados antes de reembaralhar, recomendo o seguinte:

- Para 1 maço, reembaralhe sempre que tirar uma carta;
- Para 2 maços, reembaralhe ao tirar a segunda carta;
- Para 3 maços, reembaralhe ao tirar a terceira carta;
- Para 4 maços, reembaralhe ao tirar a terceira carta (também)

Ou seja, até 3 maços faz sentido. Quatro já é demais (mesmo porque manusear 192 cartas não deve ser fácil). Mas no fim das contas, se você pretende criar senhas DWD12 uma vez ou outra, vale mais a pena utilizar 1 ou 2 maços e reembaralhar sempre!

Coringa ou K (Rei): -

A (Ás): 1

2 a 10: vale o número da carta (2 a 10)

J (Valete): 11

Q (Rainha): 12

Usando Tecnologia

Se as soluções analógicas (que em tendem a ser realmente aleatórias) não estão acessíveis, você pode utilizar soluções digitais. Existem aplicativos que simulam rolagem de dados virtualmente para qualquer dispositivo. Procure por “dice roller” que certamente encontrará. Para GNU/Linux, por exemplo, tem o rolldice, que funciona em terminal mesmo. Qualquer coisa, você pode recorrer ao site random.org ou pode fazer uma busca por “roll 1d12” no buscador do pato.

Esteja atento, porém, para duas coisas:

- Se houver como alguém ter acesso à sequência de tomos que você utilizou (para sorteá-los) e aos resultados todos das rolagens, na ordem, a sua senha poderá ser descoberta a partir dessas informações;
- Aleatoriedade em computadores não é 100% aleatória, apesar de, para humanos, virtualmente chegar bem perto.

Assim sendo, recomendo que tente uma solução que permita rolar vários dados de uma vez e que mostre o resultado sem somá-los. Assim, você escolhe mentalmente que resultado aproveitará, manda rolar 12 dados de 12 faces e escolhe o resultado na posição que tinha definido.

Por exemplo, você pensa “Escolherei o último resultado” e executa o comando “rolldice -s 12d12” em GNU/Linux. O comando mostra: “Roll #1: (12 8 6 7 2 10 3 9 2 10 12 7) = 88”. Você pensa: “Ok, o resultado que vale é 7. Vamos rolar de novo. Dessa vez escolherei o terceiro resultado” e continua.

Claro, se você não for tão paranoico, simplesmente role os dados de um em um e vá anotando e utilizando os resultado. Caso utilize um programa interativo para rolagem, talvez seja uma boa ideia encerrá-lo e reexecutá-lo após alguns lances para renovar o número-semente do algoritmo de sorteio, para prevenir caso o programa utilize um algoritmo fraco.

Usando 1 moeda

Se não tiver em mãos nenhum desses componentes para gerar números aleatórios entre 1 e 12, você pode recorrer a moedas. Precisará jogar quatro moedas. Se quiser poupar tempo, pode usar 4 moedas diferentes e atribuir a cada uma um papel. Ou poderá jogar uma só quatro vezes. Duas delas serão divisoras (Divisora 1, Divisora 2) e as outras duas serão, juntas, a contagem (Contagem 1, Contagem 2). Lembrando que, em moedas, Cara é o lado que apresenta o valor, enquanto Coroa é a ilustração (que antigamente era mesmo em referência à Monarquia, mas hoje é um rosto, o que termina confundindo os termos).

Para entender a proposta, a primeira moeda delimita se o intervalo é 1-6 ou 7-12; a segunda divide novamente. Se estava entre 1 e 6, esta moeda definirá se está entre 1-3 ou 4-6. As outras duas moedas formarão um número binário de dois bits, ajudando a sortear entre 3 números, com um 4º número que não será usado (sempre que sairem 2 coroas na contagem, o resultado será ignorado e você jogará de novo as duas moedas de contagem). Veja a tabela de auxílio:

```
 1. ## ##    2. ## #@      3. ## @#
 4. #@ ##    5. #@ #@      6. #@ @#
 7. @# ##    8. @# #@      9. @# @#
10. @@ ##   11. @@ #@     12. @@ @#
             #: cara     @: coroa
```

Senhas Curtas

1) Siga o procedimento normal de sorteio de palavras do DWD12, mas sorteie apenas uma palavra.
2) Caso tenha menos que 5 letras, sorteie uma outra palavra e junte com a anterior.
3) Caso tenha mais de 9 letras, escolha apenas as 9 primeiras (ou, se preferir, as 9 últimas ou outro segmento de 9 letras).
4) Sorteie e aplique 3 modificações aleatórias.
5) Caso a senha lhe pareça simples demais, vá sorteando outras modificações até ficar satisfeito.

Modificações Aleatórias

1 Apagar

1. a 1ª letra
2. a 2ª letra
3. a 3ª letra
4. a 4ª letra
5. a 5ª letra
6. última letra
7. penúltima letra
8. antepenúltima letra
9. a 4ª do fim pro começo
10. a 5ª do fim pro começo
11. 1 vogal à escolha
12. 1 consoante à escolha

2 Duplicar

3 Substituir por algum caractere especial à escolha ($@!#&*...)

4 Substituir por número

5 Tornar Maiúscula

10 Trocar pela próxima letra no alfabeto

11 Trocar pela letra anterior

9 Substituição

1. 1 vogal por outra
2. 1 consoante por outra
3. acentuar 1 vogal
4. consoante por arcaica
5. 1 letra por um número
6. 1 letra por um símbolo
7. 1ª sílaba por outra
8. 2ª sílaba por outra
9. última sílaba por outra
10. penúltima sílaba
11. sílaba do meio
12. Inverter toda a palavra

6 Acrescentar número

1. antes da 1ª letra
2. antes da 2ªletra
3. antes da 3ªletra
4. antes da 4ªletra
5. antes da 5ª letra
6. após a última letra
7. após a penúltima letra
8. após a antepenúltima letra
9. após a 4ª do fim para o começo
10. após a 5ª do fim para o começo
11. no meio da palavra
12. escolha a posição e o número

7 Acrescentar caractere especial

8 Trocar letras

TF: de trás pra frente

1. 1ª com a 2ª
2. 2ª com a 3ª
3. 3ª com a 4ª
4. 4ª com a 5ª
5. 5ª TF com a 4ª TF
6. 4ª TF c/a antepenúltima
7. Antepenúltima c/penúltima
8. Penúltima c/última
9. 1ª com a última
10. 2ª com a penúltima
11. 3ª com a antepenúltima
12. 4ª com a 4ª TF

12 Mover

1. 1ª letra para o final
2. 2 1ªs letras para o final
3. 3 1ªs letras para o final
4. última letra para o começo
5. 2 últimas para o começo
6. 3 últimas para o começo
7. todas vogais pela próxima
8. todas vogais pela anterior
9. 1ª vogal repetida
10. 1ª consoante repetida
11. vogal única por uma outra
12. consoante única por uma

 # Número

1. 0
2. 1
3. 2
4. 3
5. 4
6. 5
7. 6
8. 7
9. 8
10. 9
11. 2 nºs
12. Sinal + Nº

! Especiais

1. branco ou _
2. - ou +
3. . ou ,
4. ! ou ?
5. = ou *
6. \ ou /
7. ~ ou ^
8. < ou >
9. : ou ;
10. # ou “
11. @, %, & ou $
12. (,), [,], { ou }