

Lockpicking: A arte de abrir Cadeados e Fechaduras

INTRODUÇÃO	1
PARTE TEÓRICA	1
FERRAMENTAS.....	4
<i>A ferramenta de Torque:</i>	4
<i>Ferramenta “Pick”:</i>	4
ATIVIDADE	6
<i>Passo a Passo:</i>	7
ESTRUTURA DA FECHADURA DO TP(TELEFONE PÚBLICO)	8
ESTRUTURA DO CADEADO	9
PINOS DE SEGURANÇA	10
TÉCNICAS	11
CONCLUSÃO	11

Introdução

Primeiramente, muitos podem estar perguntando qual a utilidade de abrir cadeados ou fechaduras se ninguém quer ser bandido ou correr o risco de ser preso.

Conhecimento nunca é demais, e não há problema algum em saber algo como o lockpicking, não é crime e um dia quem sabe estas técnicas podem lhe ser útil.

Aparentemente pode não ter sentido escrever um texto desses para um grupo relacionado a computadores, mas é importante lembrar que computadores são equipamentos e precisam ser guardados em algum local, assim como o cabeamento de rede destes e todos os outros dispositivos.

E ao contrário do que muitos pensam, o mundo underground não vive só de conexões remotas, mesmo porque estas nem sempre nos dão o acesso necessário pra um trabalho bem feito.

Existem dezenas de encontros pelo mundo de hackers e eu diria que 80% ao menos tem uma seção para lockpicking, como no caso da HackFest, Defcon com inclusive desafios entre grupos.

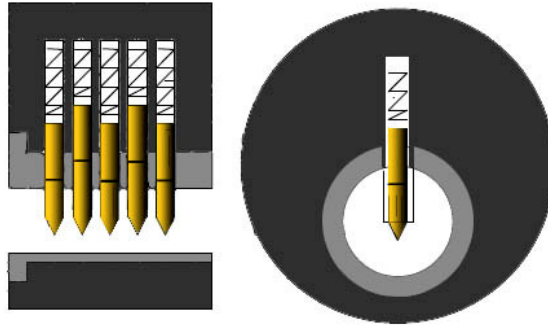
Além disso, em muitos momentos esta técnica pode ser útil, para abrir arquivos (daqueles de ferro com um monte de pastas), salas, telefones públicos, Caixas de Distribuição Geral (as caixas de prédios onde ficam todo cabeamento telefônico do mesmo).

Você já deve ter pensado no que se pode fazer com todas essas coisas, principalmente com as linhas telefônicas né.. e eu não me refiro à trote.

Parte teórica

Para aprender como abrir fechaduras e cadeados, primeiramente é necessário saber como eles funcionam. Isto poder ser a princípio cansativo e repetitivo, mas é de grande importância.

O princípio de funcionamento de fechaduras e cadeados é o mesmo.



O sistema é composto de molas, e pares de pinos. No caso do da figura acima são 5 cavidades, 5 molas, 10 pinos, 1 cilindro e a “casca” onde fica tudo isso dentro.

As molas exercem uma força sobre os 5 primeiros pinos pinos que tem a base reta. Estes por sua vez exercem força sobre os outros 5 pinos com 1 base reta e outra cônica (arredondada), isto pode ser visto facilmente, tanto no desenho quanto na foto abaixo.

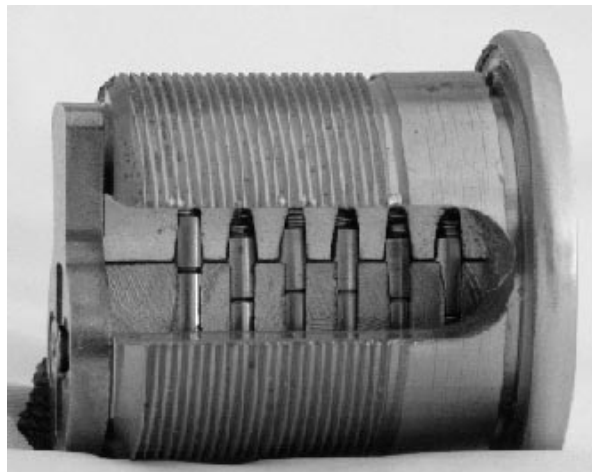


Pino com base reta e outra arredondada

Obviamente a parte arredondada do pino fica pra baixo onde a chave vai entrar, acho que não é preciso explicar o porquê. Obviamente se for em qualquer outra posição, existe grande chance da chave ficar presa ou mesmo não entrar, além de um desgaste excessivos nos pinos e na chave.

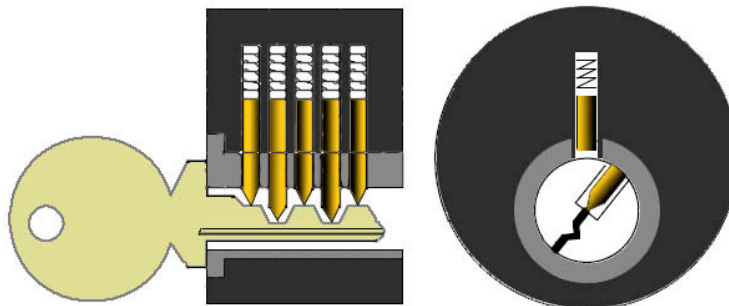
A parte cinza mais clara do desenho é o cilindro, parte móvel da fechadura, que gira quando a chave entra, mas porque ele gira com a chave e não gira sem ela ou com a errada.

Este é o princípio básico da fechadura, os pinos nem sempre possuem o mesmo tamanho e nem as molas são iguais. Isso quer dizer que se você abrir um cadeado e perde a posição dos pinos ou molas, vai ser muito mais difícil coloca-los novamente no lugar, e impossível se você não tiver mais a chave.



*Portanto, cuidado se for abrir algum cilindro.
Nesta foto é possível ver perfeitamente 12
pinos em 6 cavidades e as 6 molas*

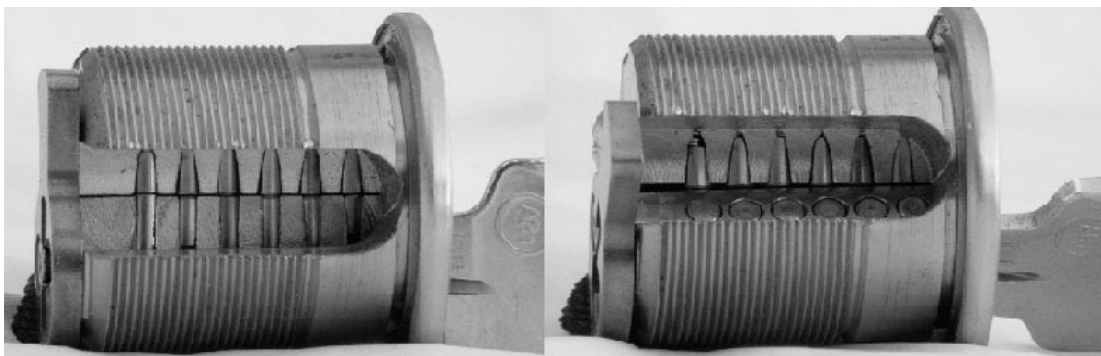
Estes pinos podem se movimentar livremente no sentido vertical dentro dos orifícios, caso sejam empurrados com uma força contrária e maior do que a força que a mola exerce, fazendo a mesma comprimir.



Assim que a chave é colocada no cilindro, como podemos ver na figura a seguir: As ranhuras da chave fazem os pinos se alinharem. Ou seja, 1 pino de cada orifício fica acima dos limites do cilindro e outro fica abaixo e isto se repete em cada orifício.



Nesta foto podemos ver o primeiro pino de cada par alinhado assim que a chave é introduzida. Deste modo o cilindro pode girar dentro da casca.



Esta foto mostra claramente os pinos alinhados, a divisão da casca mostra eles ficam alinhados perfeitamente para que possa haver o giro do cilindro.

Assim, podemos perceber que, o cilindro não girava porque os pinos impediam este movimento, com a chave no lugar eles se alinham e não travam mais o movimento do cilindro.

Já no caso de uma chave errada, realmente ela pode entrar no cilindro, e isto não quer dizer que ela vá servir. O fato de ela entrar quer dizer que o modelo de chave é o mesmo, mas não o segredo.

O modelo é basicamente o padrão de tamanho da mesma, já o que faz os pinos se alinharem é o segredo, e em teoria é único por fechadura, obviamente podendo existir fechaduras para a mesma

chave como no caso de algumas salas em escritórios e telefones públicos, onde cada modelo de equipamento possui um segredo. Já que seria inviável uma chave pra cada orelhão na cidade.

As fechaduras mais simples e as que no caso nós vamos encontrar nesses locais tratados na introdução seguem o funcionamento básico descrito acima.

Ferramentas

O uso de ferramentas específicas para este trabalho é recomendado caso você queira ser um chaveiro ou então um profissional na área, mas como acredito que não seja o objetivo da maioria é preciso arranjar ferramentas sem grande custo.

Nesse caso eu criei minhas próprias ferramentas de acordo com as minhas necessidades, claro que não ficaram bonitas, mas pra o meu objetivo é suficiente.

Para trabalhar com fechaduras simples e cadeados, apenas 2 ferramentas são necessárias. A ferramenta de torque e a ferramenta pick

A ferramenta de Torque:

Esta ferramenta dará o giro ao cilindro, portanto precisa ser um pouco resistente. No meu caso eu usei um arame relativamente grosso. Fiz um gancho com o alicate e lixei a ponta (parte mais clara) para que ele entre na fechadura.



Estas imagens representa a minha ferramenta de torque

Ferramenta “Pick”:

Para esta, que será propriamente a ferramenta que vai mexer com os pinos, eu usei um grampo de cabelo também lixado, à partir da linha pontilhada, para entrar perfeitamente no lugar da chave.



Estas imagens representa a minha ferramenta pick.

Ferramentas ruins nos deixam na mão, podem quebrar, empenar ou mesmo não serem adequadas pra um determinado tipo de fechadura. Isto tudo nos faz perder tempo, e é o que menos queremos quando estamos desprotegidos olhando pra uma fechadura. Portanto, cuidado nisso.



Nesta foto acima, podemos ver um “set” básico para o lockpicking.

As duas ferramentas em cima da foto são feitas para dar o torque ao cilindro, as outras são as pick usadas para várias fechaduras diferentes.

Um set como esse abre uma gama impressionante de fechaduras e é mais do que suficiente pro que queremos.

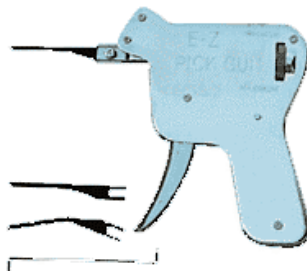
As mais comuns são a 1, 2, 6 e 7 de cima pra baixo. As de torque que são sempre necessárias e o tamanho delas também é fundamental já que existem cadeados de vários tamanhos.

A 6 e 7 conhecidas como Rake e Half Diamond e servem pra casos mais gerais, fechaduras comuns e simples, as outras são mais avançadas.

Existe pela internet um vídeo criado pelo PYRO1234321 se não em engano que ensina a criar suas próprias ferramentas à partir de uma simples lâmina, dessas de serra. Muito interessante e barato.

Outra ferramenta muito difundida é a ferramenta elétrica, ela funciona impulsionando os pinos pra cima várias e várias vezes automaticamente, fazendo com que “pulem” dentro do orifício, sem a necessidade do trabalho todo de levantar um por um.

O problema da ferramenta é a agressividade dela, facilmente você pode perder fechaduras se não tiver prática e paciência.



Ferramenta elétrica. A ponta sobe e desce rapidamente, à partir do acionamento do gatilho empurrando pinos pra cima, até travarem no cilindro

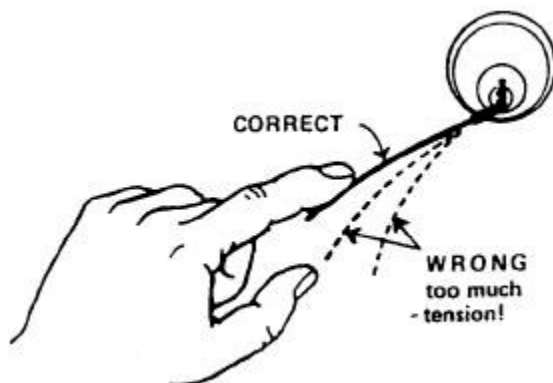
Existem milhares de ferramentas para lockpicking, muitas específicas, servindo apenas pra um tipo de fechadura, mas isso é assunto pra outros textos.

Atividade

Na maioria dos filmes de ação existe alguma cena do mocinho abrindo a porta com um grampo de cabelo, clips e coisas do tipo. De fato, isto não é impossível, mas requer bastante prática.

Alguns devem estar pensando em como alinhar de uma vez todos os pinos. De fato alinhar todos ao mesmo tempo seria o ideal, mas impossível sem uma chave. Então o que faremos é alinhar, a grosso modo, 1 por 1 até a abertura da fechadura.

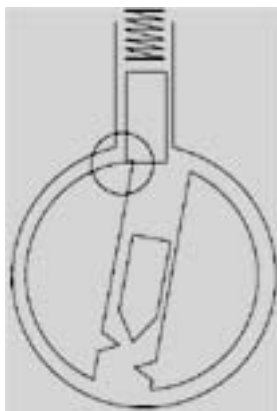
Se tentarmos girar um pouco o cilindro, sem forçar muito, veremos que existe uma folga. Esta folga é a folga do pino dentro do orifício, pra ele não ficar apertado podendo travar ou bloquear o giro do cilindro.



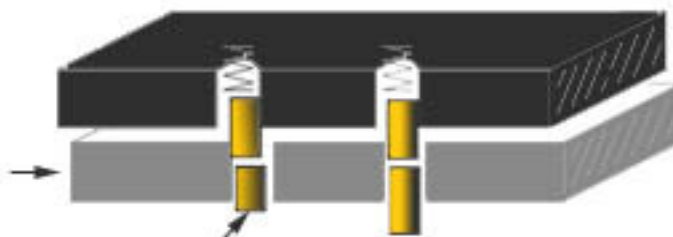
Observe que uma pequena tensão apenas é indicada, e ela deve ser feita durante toda o arrombamento.

Girar muito o cilindro vai fazer com que os pinos fiquem presos na parede da casca ou do próprio cilindro, travando o mesmo, dificultado e talvez até impossibilitando nosso arrombamento.

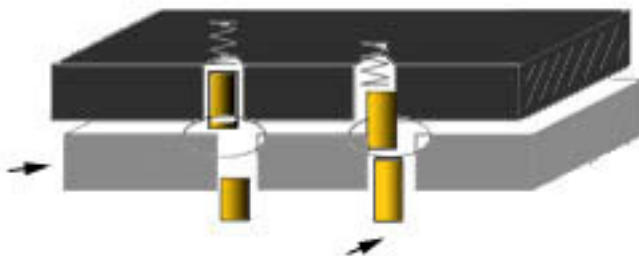
O que vamos fazer é tirar essa folga do pino e cilindro tentando fazer com que ele trave na ponta do cilindro como visto na figura abaixo.



Pino preso na ponta (limite) do cilindro, assim que todos estiverem nessa posição, a fechadura estará aberta



Força de torque e elevação do pino 1 ao limite do cilindro



Continuando a força de torque e pino 1 preso no limite do cilindro, elevação do pino 2 ao limite do cilindro

Passo a Passo:

- 1- Force a ferramenta de torque no sentido da abertura da fechadura até perder a folga, mas não force demais, isso irá fazer o pino ficar preso com o atrito e nada então vai movê-lo
- 2- Introduza a ferramenta “pick” e eleve o pino ao final do orifício. Você perceberá que ele ficou preso quando o pino de baixo, estiver livre dentro do cilindro.
- 3- Faça isso com os outros pinos mantendo a pouca força na ferramenta de torque.

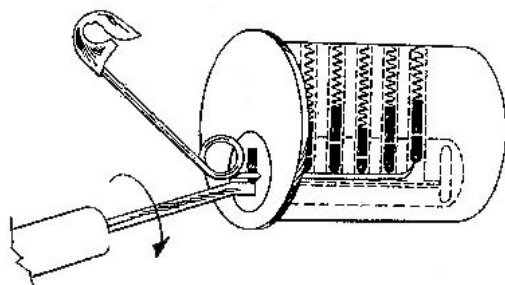


Figura 1

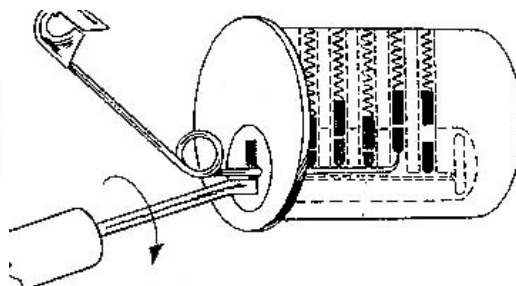


Figura 2

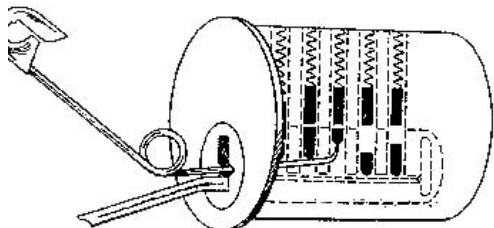


Figura 3

A ferramenta de toque deve estar sempre com uma leve tensão, assim que os pinos estiverem alinhados ela vai girar o cilindro automaticamente.

Isto é tudo para que a fechadura se abra. É provável que no começo não se obtenha sucesso, seja pela escolha errada da ferramenta ou muita força na ferramenta de torque, o que é um erro comum.

Estrutura da Fechadura do TP(Telefone Público)

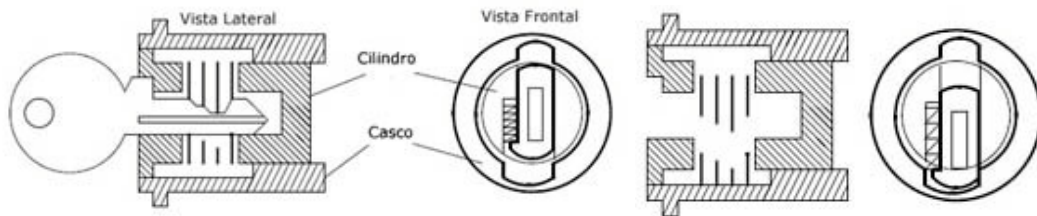
Existem alguns tipos de fechaduras e as principais atualmente são os modelos com chave-tetra e chave simples.

O modelo de chave tetra não será explicado pela necessidade de equipamentos um pouco mais sofisticado do que as minhas ferramentas feitas em casa com arame, mas o funcionamento é basicamente o mesmo só que são 2 segredos numa mesma chave.

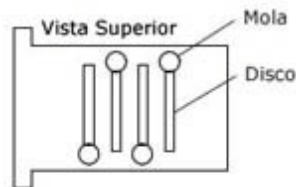
A chave tetra são 4 chaves juntas em uma, mas na verdade são 2 segredos as outras 2 chaves são cópias.



Estes discos juntos fazem o segredo a fechadura, eles vão posicionados nos espaços específicos como pode ser visto na vista superior do cilindro.



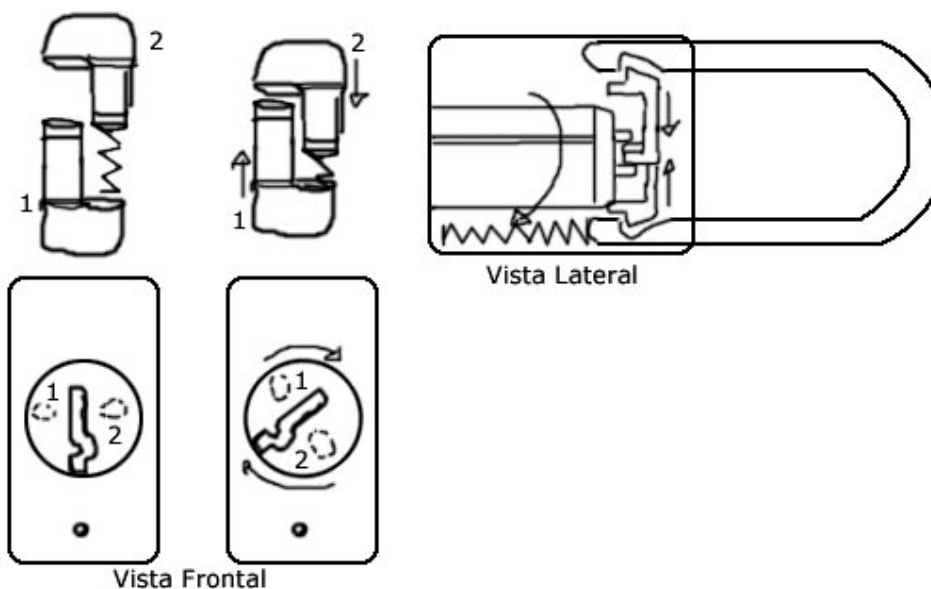
Na vista lateral as linhas pretas dentro do cilindro representa os discos e o espaço branco entre elas o espaço de dentro do disco, por onde a chave irá passar.
Se os discos forem alinhados, o cilindro gira e a fechadura abre.



Nesta figura podemos ver a disposição dos discos e das molas numa vista superior.

Estrutura do cadeado

Como já visto na parte teórica, o cadeado segue exatamente aquela imagem, mas ainda falta um detalhe. Como ele é um bloco, falta explicar o funcionamento mecânico para a abertura do mesmo.



Com muita boa vontade vocês serão capazes de entender o mecanismo do cadeado. Basicamente o sistema é composto de 2 peças e o cilindro. Atrás do cilindro são encontrados 2 pinos, mostrados pela lista pontilhada na vista frontal.

Duas peças estão em constante contato com estes pinos, são as peças 1 e 2, e estas peças prendem a travas da tranca metálica. A mola encaixada na peça 2 faz com que o sistema fique o tempo inteiro esticado até que o cilindro gire e as peças 1 e 2 sejam empurradas em direções opostas (vide vista frontal no giro) fazendo com que o sistema se comprima, abrindo a tranca.

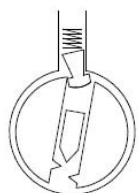


Já que o intuito é fazer com que o sistema se comprima pra largar as travas como mostrado na vista lateral, porque não colocar algo pela própria tranca e tentar chegar na aba da trava? Este é o princípio do chamado “padlock shim”.

Basta simplesmente encaixar a aba na entrada da tranca e empurrar. Obviamente o espaço não é grande, mas não é tão difícil.

Pinos de Segurança

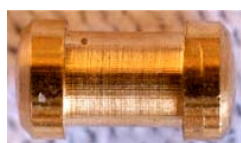
Os pinos de segurança nada mais são do que pinos com algum formato especial visando dificultar o lockpicking, pelo menos os arrombamentos feitos por leigos.



Veja na figura abaixo o exemplo de funcionamento de um pino de segurança. Eles estão prendendo o cilindro e ainda por cima deixando o arrombador pensar que está tendo ou que teve êxito com o relativo giro da ferramenta de toque.



Este pino é o pino padrão, normalmente encontrado em fechaduras e cadeados e não possui qualquer formato especial para evitar o lockpicking. O arrombamento com pinos lisos é muito simples.

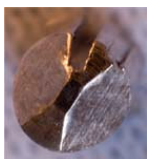


Pinos Superiores, Os pinos superiores normalmente não são muito complicados, e são encontrados em vários cadeados e fechaduras.

O importante é não deixar que a ferramenta de torque entre na ranhura, isso vai travar o cilindro e para reverter tal situação, você irá precisar voltar a ferramenta de torque um pouco até ouvir um estalo e torcer para que seja esse pino, ou então reiniciar o arrombamento. Não há grandes problemas no arrombamento manual.



Os pinos serrilhados são bastante complicados de se efetuar o pick manualmente. As ranhuras nos iludem achando que o pino ficou preso direito, mas normalmente o limite do cilindro prende numa destas ranhuras e acaba por falhar toda a nossa tentativa. Alguns cadeados, como os americanos, possuem o serrilhado em todos os pinos, tanto nos de cima como nos de baixo. O uso de ferramentas elétricas para o arrombamento é recomendado.



Este é um dos pinos mais complicados de se posicionar, eles não apenas têm a ranhura atrás, perto do segundo pino, como também têm um serrilhado lateral e uma ponta especial, como podem ver na primeira imagem.

Isto permite que a chave gire o pino quando introduzida, posicionando-o da única maneira possível para o encaixe perfeito no orifício e na altura perfeita para o alinhamento.

Técnicas

Um método que funciona comigo é posicionar a ferramenta de torque, sem fazer muita força, isto poderia deformar o pino. Força suficiente apenas para tirar a folga da fechadura.

Pressionar todos os pinos pra cima com o “pick”, e quando eles retornarem é possível que fiquem presos e a tranca se abra, com esta técnica eu abro cadeados PAPAIZ CR 25 em cerca de 3 segs. ou menos.

Outra técnica é posicionar a ferramenta de toque da mesma maneira, e usar a ferramenta “pick” pra cima e pra baixo fazendo com que novamente os pinos fiquem presos e a tranca se abre.

Existem ferramentas elétrica que fazem este mesmo movimento, e você até pode fazer uma bem simples com esse motorzinho de carrinho elétrico com um pequeno peso no eixo, fora do equilíbrio, pra quando o motor girar a inércia forçar o conjunto a subir e descer.

Como nessas escovas de cabelo que fazem massagem, vibram...

Para aprender mais sobre isso, mandem-me um e-mail ou então procurem no eMule textos sobre lockpicking, eu estou disponibilizando mais de uma dezena de textos pdf e vídeos.

Conclusão

O lockpicking é relativamente simples, mas muita prática é necessária. Espero ter ajudado.

Texto escrito por BackBone

Algumas imagens foram retiradas do texto sobre Lockpicking do MIT e coloridas por BackBone