

Apostila de Chaveiro

A maioria das pessoas carregam 5 (cinco) a 10 (dez) chaves com elas, sempre que saem. Em seu anel porta chaves, você pode ter várias chaves para a casa, um ou duas, para o carro e algumas para o escritório ou casa de um amigo.

Seu anel porta chaves é uma demonstração clara da tecnologia justa que se faz aos cadeados. Você provavelmente interage com dúzias de cadeados todos os dias. A razão principal de nós usarmos cadeados em toda parte é que eles nos fornecem um sentido de segurança. Más em filmes de cinema ou televisão, espiões, detetives e assaltantes podem abrir um cadeado ou fechadura, muito facilmente, às vezes usando só um par de cliques. Isto é simples e podemos dizer; será que é possível, alguém abrir um cadeado assim; tão facilmente??

Neste artigo, vamos aprender na teoria e prática, o funcionamento dos cadeados ou fechaduras, vamos explorar esta tecnologia fascinante e aprender todos os segredos desta arte, inclusive, abrir fechaduras com um simples Clipe...

Cadeados e Chaveiros

Cadeados podem ser abertos com a manipulação de uns simples componentes (clipes, michas, grampinho de cabelo, etc), poderemos abrir cadeado ou fechadura sem usar Chave.

Entender o funcionamento é o ponto principal. Então, primeiramente você tem que saber, como os cadeados e às chaves funcionam.

Os cadeados existem de todas formas e tamanhos, com muitas variações inovativas dos projetos. Podemos receber uma idéia clara do processo de funcionamento de cadeado observando um exemplo simples na figura abaixo. A maioria dos cadeados são baseados em conceitos claramente semelhantes.



Um cadeado normal ou fechadura: Quando vira-se a chave, o parafuso desliza num entalhe do batente(armação) da porta.

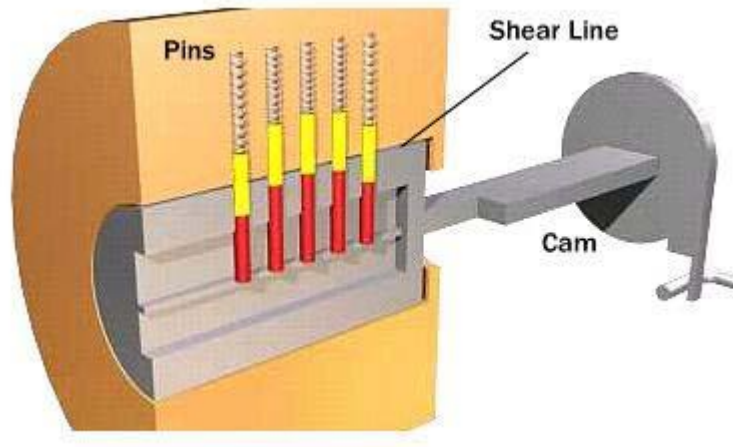
Para a maioria de nós, o cadeado bem familiar é os cadeados normais do tipo fechadura (morto-parafusos) que você pode achar numa porta principal. Olharemos este tipo de cadeado explicaremos como funcionam estas fechaduras.

Os Pinos é o Segredo

A maioria das fechaduras de portas ou cadeados são de Cilindro (tambor). Na fechadura (cadeado) de Cilindro, a chave vira um Cilindro, Conhecido também com Tambor; que vira um dispositivo unido a uma lingueta. Quando o Cilindro é virado meia volta, o dispositivo puxa a trava e a porta é destrancada. Quando o Cilindro (tambor) faz o sentido inverso, o cam libera o parafuso e a mola estala-o em lugar então a porta não pode abrir. Num cadeado de deadbolt, não há nenhuma mola mecanismo -- o cilindro de desvio desliza o parafuso adiante e atrasado. Um deadbolt é mais seguro que um trinco desde que é muito mais duro empurrar o parafuso no lado da porta.

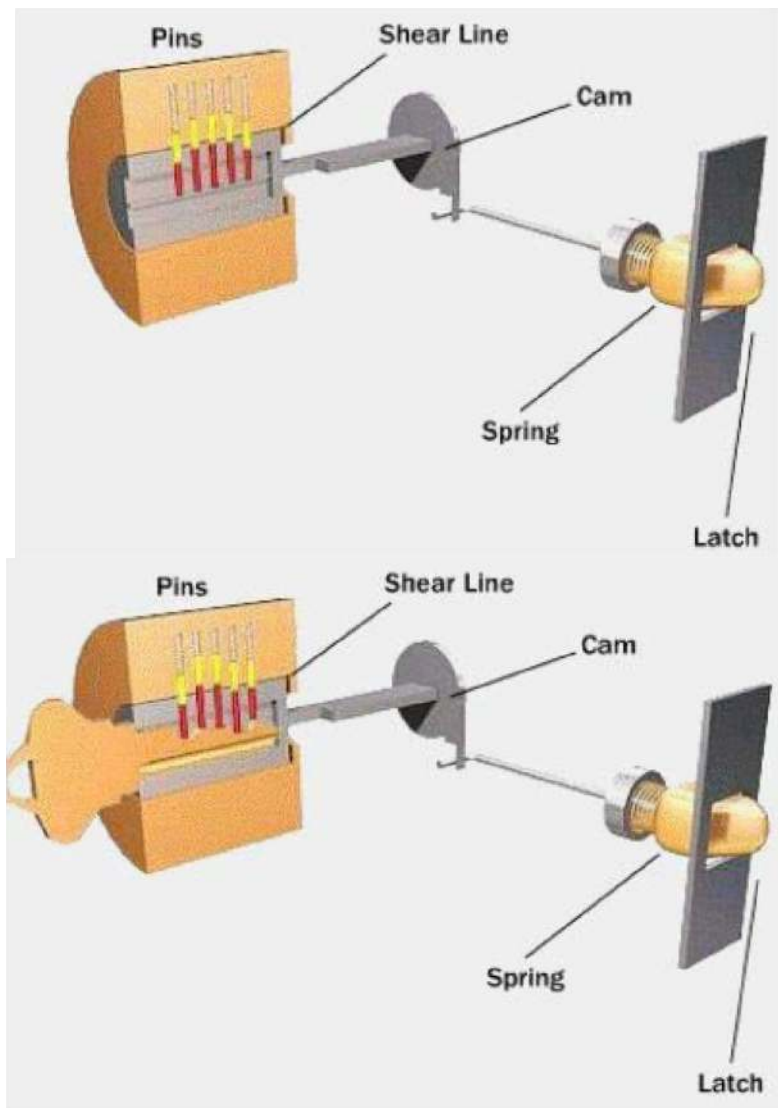
Dentro de um cadeado de Cilindro (tambor), há um tipo de quebra-cabeça, que só a Chave correta poderá resolver. A variação principal em projetos de

cadeado é a natureza deste quebra-cabeça. Um dos quebra-cabeças bem comuns é o "Pino-Cilindro e Corpo", mostrado embaixo.



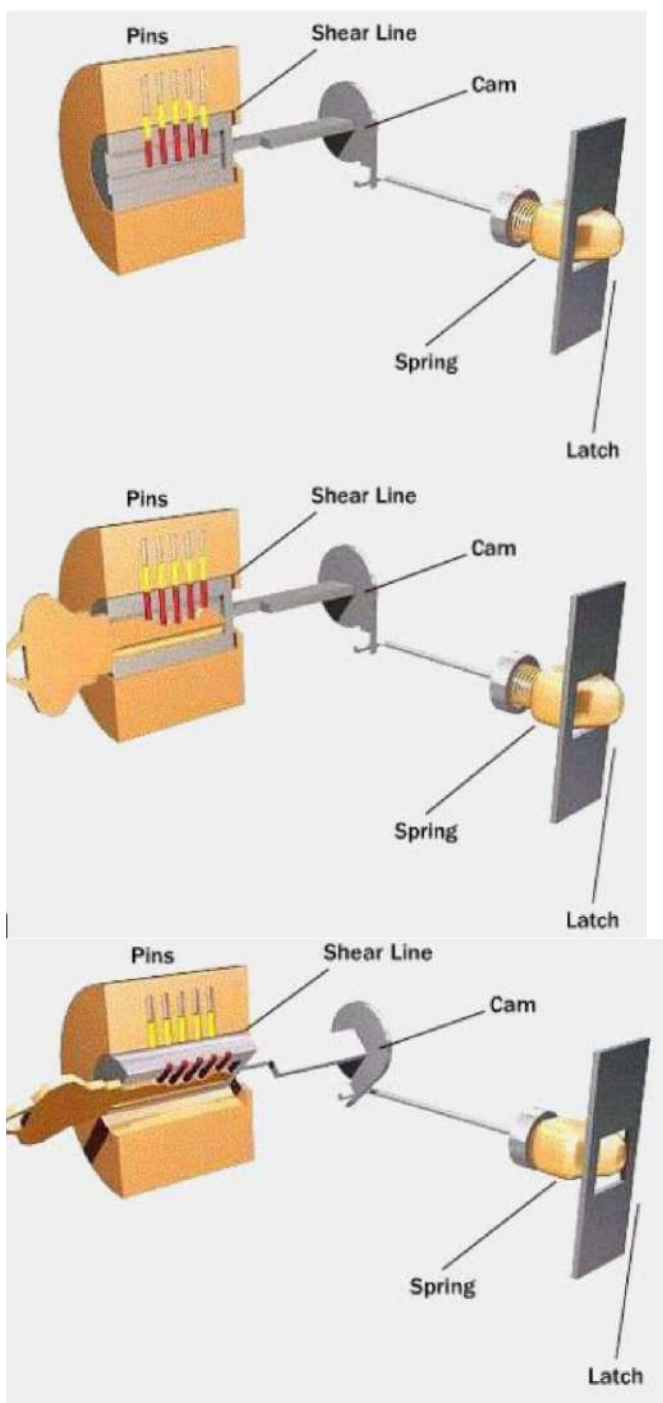
Os componentes principais no pino-e-projeto de copo são uma série de Pinos pequenos de comprimento variável. Os Pinos são divididos em pares. Cada par descansa num eixo horizontal que percorre a parte central do Cilindro. As molas no topo dos Pinos Superiores, mantém os pares de Pinos em posição no Cilindro (tambor). Quando nenhuma chave é inserida, o Pino Inferior de cada par está completamente dentro do Cilindro (tambor), enquanto o Pino superior está incompleto (entre o cilindro e o corpo) meio no Cilindro e meio na Caixa, à posição destes Pinos Superiores mantêm o Cilindro em desvio. Os Pinos unem o Cilindro à Caixa. Aqui está como trabalha:

Quando insere uma Chave, a série de entalhes na Chave empurra os pares de Pinos (inferiores e superiores) até o nível da "Linha de Corte". Se a Chave for incorreta, empurrará os Pinos de modo que a maioria dos Pinos Superiores, ficarão com uma parte no Cilindro e a outra parte na Caixa (corpo do cadeado), travando eficazmente o Cilindro. Na ilustração abaixo, os Pinos Superiores são os de cor amarela. Veja na figura, o que acontece ao inserir uma Chave incorreta.

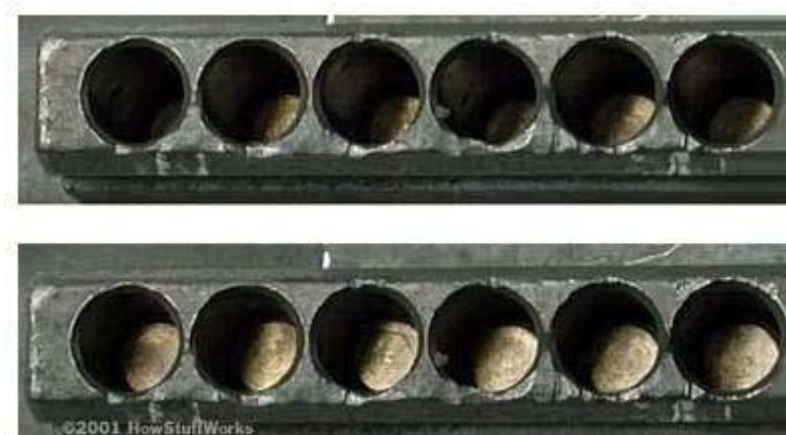


A chave sendo correta empurrará cada par de Pinos para cima o suficiente de modo que o ponto onde os dois Pinos venham a alinhar-se perfeitamente com o espaço entre o Cilindro e a Caixa (corpo), este espaço é chamado de "Linha de Corte". Pôr outro meio, a Chave empurrará os Pinos para cima de modo que todos os Pinos Superiores serão inseridos completamente na Caixa; enquanto todos os Pinos Inferiores descansam completamente no Cilindro (tambor).

Não havendo qualquer Pino, unindo o Cilindro com à Caixa, então este moverá livremente, e empurrará o parafuso (Spring) para fora, desta maneira, a porta será destrancada. Veja na figura, o que acontece quando inserir a Chave correta.



Este projeto simples de quebra-cabeça é muito eficiente. Desde que os Pinos estão escondidos dentro do cadeado, está claramente difícil para a maioria das pessoas mover o Cilindro (tambor) sem a Chave. Más, com muita prática, é possível resolver o quebra-cabeça por outro meio.

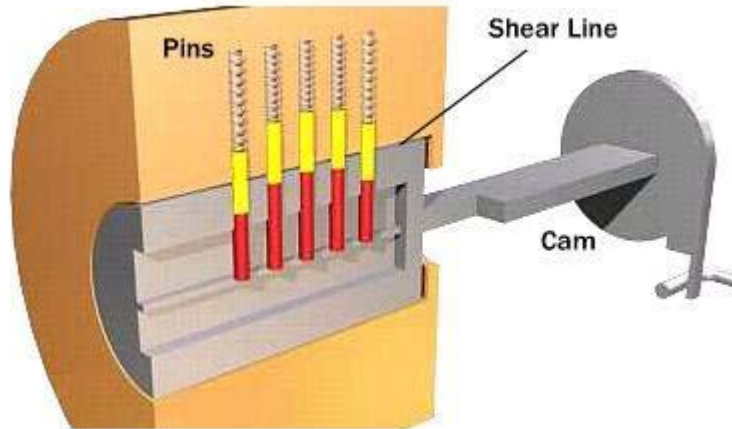


Quando a chave correta é inserida os Pinos sobem até o nível da "Linha de Corte"

Os Pinos é quem da Segurança

Quando o Cilindro (tambor) vira o outro meio, o cam libera o parafuso e a mola trava-o no lugar então a porta não pode abrir. Num cadeado de deadbolt, não há nenhuma mola mecanismo - o Cilindro de desvio desliza o parafuso adiantando e atrasando. Um deadbolt é mais seguro que um trinco mola-guiado desde que é muito mais duro empurrar o parafuso do lado da porta.

Dentro de um cadeado (fechadura) de Cilindro, há um tipo de quebra-cabeça, que só a chave correta pode resolver. A variação principal em projetos de cadeados é a natureza deste quebra-cabeça. Um dos quebra-cabeças mais comum e fácil de encontrar é o de Pinos que fica no Corpo do cadeado e do Cilindro.



Os componentes principais no projeto de um cadeado, são uma série de Pinos pequenos de comprimento variável. Os Pinos são divididos para cima em pares. Cada par descansa num eixo existente no centro do Cilindro. As molas no topo dos Pinos mantêm, os pares de Pinos em posição no Cilindro. Quando nenhuma Chave é inserida, o Pino Inferior de cada par está completamente dentro do Cilindro, enquanto o Pino Superior está incompleto ou seja metade no corpo e metade no Cilindro (tambor) A posição destes Pinos Superiores mantêm o Cilindro travado; os Pinos unem o Cilindro e à Caixa (corpo) do cadeado.

Às Ferramentas Básicas

Nós aprendemos, que a chave correta posicionará os Pinos no corpo do cadeado, de modo que todos os Pinos Inferiores, descansam no Cilindro e todos os Pinos Superiores descansam, na Caixa (corpo) do cadeado. Ao inserir a Chave correta neste tipo de cadeado, você simplesmente move cada par de Pinos na posição correta, um por um.

Há dois elementos principais, envolvidos nestes procedimentos:

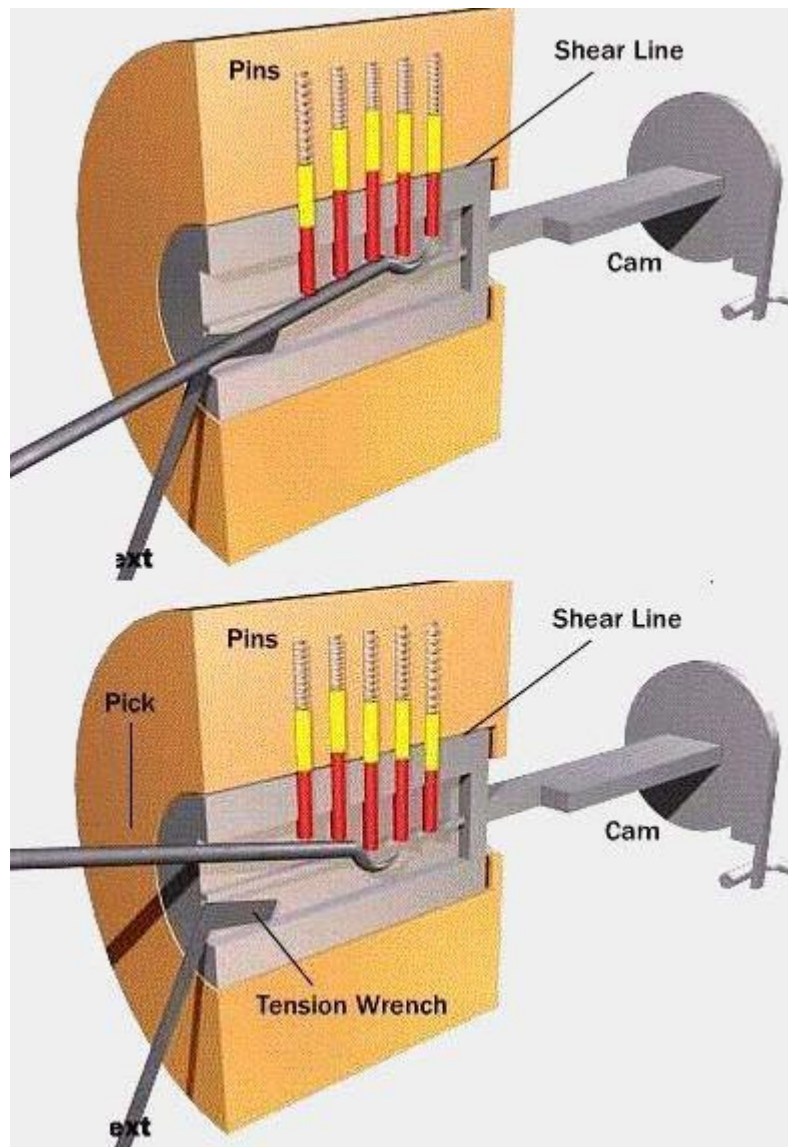
Micha Simples: - Micha simples são longos pedaços de metal, cuja ponta é curvada para cima (é semelhante à uma alavanca de obturação usada pelos dentistas). São usadas para alcançar os Pinos no cadeado e empurra-los para cima.

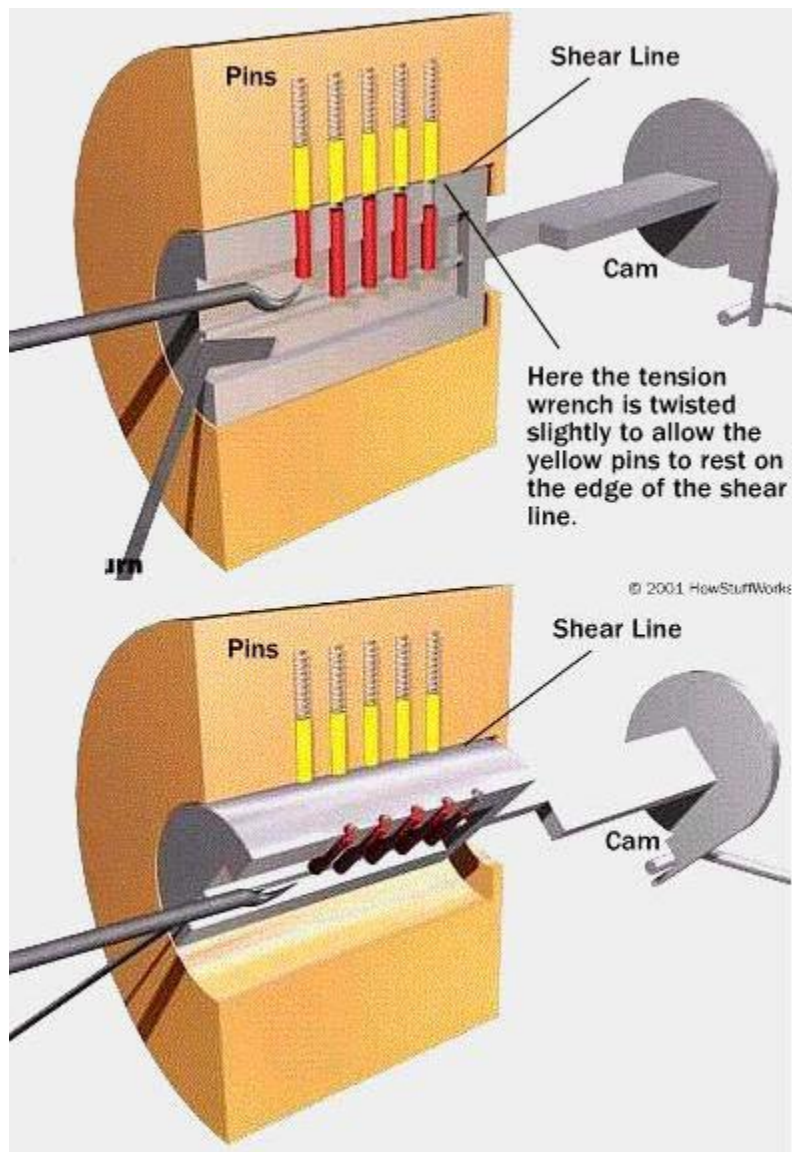
Alavanca de Tensão: - Alavanca de Tensão conhecida como virador; e às Michas, existem de diversas formas e tamanhos.

Funcionalmente, elas não são muito complexas. O tipo simples de alavanca de tensão é uma chave de fenda fina, cuja ponta é dobrada e achatada de modo que possa encaixar firmemente no orifício do Cilindro. A sua função é virar o Cilindro, assim que os Pinos forem liberados.

Técnicas de Abertura

O primeiro passo para abrir (michar) um cadeado é inserir a Alavanca de Tensão (Tension Wrench) no buraco da fechadura e virar levemente na mesma direção que você viraria a Chave. Isto força levemente o Tambor, fazendo com que os Pinos, fiquem prontos para saltarem pra dentro da caixa, assim que enfiar a Alavanca (Pick) que pode ser um clipe um grampo de cabelo, etc., desde que tenham um pequeno gancho na ponta..Veja na figura abaixo, o funcionamento da micha (Pick) junto com a Alavanca de Tensão (Tension Wrench).





Enquanto aplicar pressão no Tambor, você insere uma alavanca no buraco da fechadura e começa fazer o levantamento dos pinos. O objetivo é levantar cada par de Pinos, até o nível em que o Pino Superior mova-se completamente pra dentro da caixa, como se estivesse sendo empurrado pela Chave Correta. Enquanto se faz isto, aplica-se levemente uma tensão na alavanca de tensão, você sentem-se ou ouve um leve estalido, quando as quedas dos Pinos entram em posição. Isto é o som do Pino Superior coincidindo bem na soleira do eixo. A soleira manterá o Pino Superior preso na caixa, então não cairá novamente no Tambor.

Existe uma folga (Shear Line) infinitamente pequena, entre o Tambor Interno e a Caixa (tambor externo) da fechadura. É esta folga, que faz com que o Pino Superior encaixe na Caixa, quando damos um pequeno jogo no Tambor, usando a alavanca de tensão.

Desta maneira, você move cada par de Pinos na posição correta, até que todos os Pinos Superiores sejam empurrados completamente na caixa e todos os Pinos Inferiores descansem dentro do Tambor (cilindro). Neste ponto, o Tambor poderá ser girado livremente, fazendo o cadeado abrir.

Conceitualmente, o processo de micar cadeado é bastante simples, mas é uma habilidade muito difícil de dominar. Os chaveiros têm que aprender exatamente qual a pressão a ser aplicada e ouvir o som. Se aplicar muita pressão na Alavanca de Tensão, isto fará com que os Pinos fiquem travados na caixa e não desloquem para cima. Eles também devem aguçar seu sentido de toque ao ponto onde possam sentir-se as forças, levemente aplicadas nos Pinos, foram suficientes para desbloquearem. Adicionalmente, devem aprender imaginar (visualizar mentalmente) todas as partes dentro dos cadeados. Micar Cadeado com sucesso depende da familiaridade completa com o projeto do cadeado.

OBS: Coloque Pó de Grafite no interior da fechadura, este pó lubrifica os Pinos, fazendo eles deslizarem com mais facilidade.
Nunca use óleo em fechaduras ou cadeados.

Outra Técnica

Outra técnica de abertura muito menos precisa, mas que realmente pode ser tentada. Micar um cadeado, você insere na fechadura uma alavanca cuja ponta seja entortada ficando semelhante a um gancho. Então puxa o ganchinho para fora rapidamente de modo que pula todos os Pinos para cima em seu meio fora.

Conforme você puxar para fora o gancho, ao mesmo tempo, vire o Tambor, usando a Alavanca de Tensão,. Se os Pinos Superiores moverem para cima, alguns acontecerão de cair na soleira do Tambor.

Freqüentemente, Chaveiros começam por michar individualmente os Pinos, e então faz isto em todos os Pinos, diversas vezes, até todos eles subirem para a Caixa, destrancado o cadeado.

Fechadura de Armário

Nós já estudamos, fechaduras a Tambor Interno com Pinos, Caixa ou Tambor Externo. O Corpo do cadeado pode ser chamado de Caixa ou Tambor Externo. Acharás este tipo de cadeado em toda parte, todas as casas tem fechaduras. São tão populares porque são relativamente baratos e oferece bastante segurança. Para um típico cadeado de 5 (cinco) Pinos, é possível, usando os mesmos Pinos fazer 120 (cento e vinte) combinações, ou seja, podemos fazer 120 chaves diferentes. Más se cortarmos cada pino em 3 pedaços diferentes. Então será possível fazer 1.728.000 (hum milhão setecentos e vinte e oito mil) combinações diferentes. Considerando o número de Fábricas de fechaduras, podemos até pensar: Seria possível um ladrão ter uma Chave igual a nossa no momento de praticar o ato ???. Conforme nos mostrou o cálculo das combinações esta possibilidade é imensamente remota.



Fechadura de Tambor usada em Armários

Outro cadeado comum que também usa Tambor (cilindro) é o cadeado de Corpo Redondo. O principio de funcionamento é o mesmo. Estes cadeados tem seu Corpo unido com a tampa. Encontra-se no meio os pinos ficando fácil para

abrir. Aliás, é um pouquinho mais fácil Michar (Abrir) estes cadeados de corpo redondo porque o buraco da fechadura é mais largo.

Esta Tampa Redonda fica para fora do cilindro, unindo-a com a caixa de cadeado. As Rodas têm um buraco no centro no qual a chave assentará.



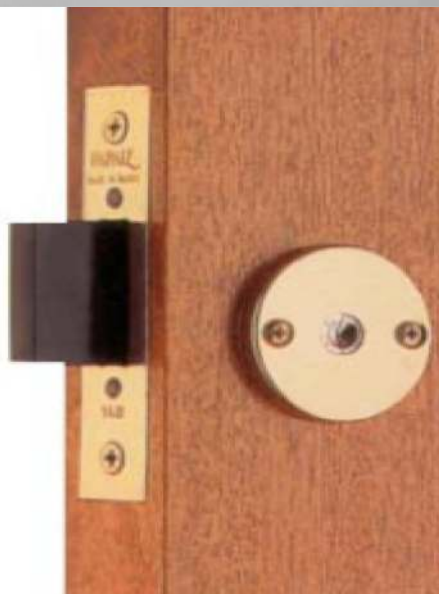
Vista de frente da Fechadura. Tampa e Cilindro

Os cadeados de Corpo Redondo, tem uma haste presa no final do Tambor. Para michar estes cadeados, aplicamos a mesma técnica já estudada. Os cadeados de Corpo Redondo, são usados em Arquivos fichários, Armários para escritório, Compartimentos e Carros, assim como em muitos projetos, em que for preciso usar uma fechadura.

Cadeado Tubular

Cadeados Tubulares, são cadeados conhecidos por usar Chave Tetra, são usados principalmente em portas de comércio. São superiores aos cadeados estudado neste curso. São também mais caros. Em vez de uma fila de Pinos, os cadeados tubulares têm Pinos posicionados ao redor de uma circunferência do Cilindro. Isto Torna-os muito mais difícil de michar. Com as técnicas

explicadas aqui, não funciona neste tipo de cadeado. Existem michas, feitas em indústria para abrir este tipo de cadeado.



Alcance das Ferramentas

O experimento nos mostrou que precisamos de algumas ferramentas básicas. O Trabalho ficará muito mais fácil se temos às ferramentas de apropriada. Precisamos ter um estojo com às ferramentas básicas ou seja, alguns cliques e uma chave de fendas, uma Alavanca de Tensão e diversas michas feitas com pedaços de serra. Estas serras são aquelas usadas para cortar ferro. Pega-se um

pedaço de uns 10 centímetros e com o auxílio de um esmeril fazemos diversos entalhes nesta serra, de modo que ela fique parecida com uma Chave.

Re-Configurar os Pinos

Uma coisa interessante sobre Fechaduras a Tambor, é que você pode re-configurar os Pinos de modo que eles assentem em uma Chave que você já possui (fornecido que a tecla é para o mesmo projeto de cadeado). As vantagens deste procedimento é óbvio: Podemos adicionar novos cadeados em nossa casa ou para comércio sem ter que carregar um punhado de novas chaves em nosso anel porta chaves.

Fazer uma nova Chave para um cadeado existente é fácil; você faz uma série de entalhes na Chave, de modo que suspenda cada um dos Pinos Superiores acima da Linha de Corte. Essencialmente, corta-se um padrão de metal que combine o padrão dos Pinos do cadeado.

Mudar o segredo de um cadeado, de modo que possa usar uma Chave já existente. Você simplesmente trabalha na direção oposta: Muda a posição dos Pinos no Cilindro (tambor) de modo que combine com as posições do entalhe da Chave. Se o cadeado é fabricado com um sistema universal de segredos, qualquer chaveiro poderá trocar este segredo em pouco tempo.



Os eixos e pinos do cadeado de corpo contem várias molas e pinos minúsculos.



A combinação correta dos pinos alinha perfeitamente com os entalhes na chave.

Para um típico cadeado de 5 (cinco) Pinos, é possível, usando os mesmos Pinos fazer 120 (cento e vinte) combinações, ou seja, podemos fazer 120 chaves diferentes. Mas se cortarmos cada pino em 3 (três) pedaços diferentes. Então será possível fazer 1.728.000 (um milhão setecentos e vinte e oito mil) combinações diferentes. Considerando o número de Fábricas de fechaduras, podemos até pensar: Seria possível um ladrão ter um Chave igual a nossa no momento de praticar o ato ?. Conforme nos mostrou o cálculo das combinações esta possibilidade é imensamente remota.

Trocando o Segredo

O processo de re-keying em um cadeado é muito simples. O chaveiro retira todos os Pinos do Cilindro. Então, aproveitando uma coleção de Pinos de substituição de vários tamanhos, o chaveiro escolhe novos Pinos, mais baixos que assentem perfeitamente entre os entalhes da Chave e a Linha de Corte. Desta maneira quando inserir uma nova Chave, os Pinos Inferiores empurrarão todos os Pinos Superiores acima da Linha de Corte, permitindo o Cilindro virar livremente. (Este processo pode variar dependendo do projeto particular do cadeado.)

Não importa se os Pinos Superiores são longos (desde que descansem acima da Linha de Corte quando a Chave for inserida), Em seguida o chaveiro simplesmente re-insere os seis Pinos Superiores originais que vieram com o

cadeado. E isso é tudo o que tem que ser feito neste processo de re-keying. O processo inteiro leva só alguns minutos.

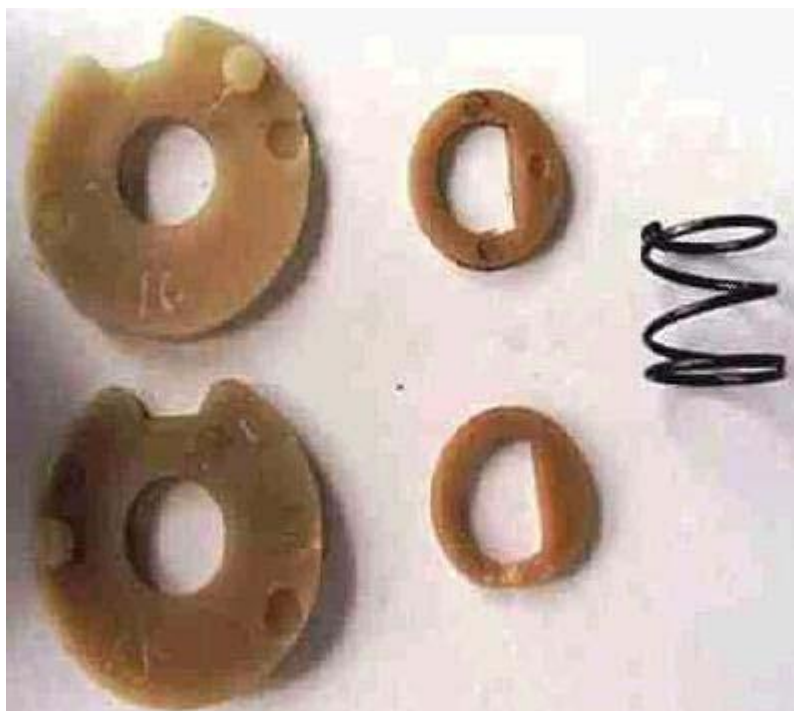
Cadeado de Combinação



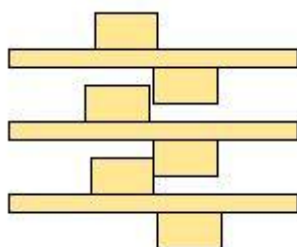
Com certeza você já viu muitas fechaduras de combinação, mas você jamais parou pensar que o que é dentro? Nesta edição vamos ver Como o Material Trabalha e destrancaremos os segredos de uma fechadura de combinação! Aqui está o cadeado que nós exploraremos:



Há três cams numa fechadura de combinação típica. Neste cadeado um do cams é metal e é ligado diretamente ao rosto de desvio do cadeado. O outro dois cams, são plástico. Há dois espaçadores plásticos que assentam entre o cams:



Assentam num eixo moldado nas costas do cadeado com uma mola pressionando a pilha de cams junto quando o cadeado é montado. A mola fornece fricção entre o cams segurá-los em lugar. O cams tem um dente em cada lado, e estes dentes empenham como o cams gira:





O propósito do cam é controlar um trinco que empenha o fim do hasp do cadeado. Cada cam tem uma entrância neles. Quando as entrâncias alinham adequadamente o trinco é capaz de assentar nas entrâncias e libera o hasp: Contrariamente o trinco empenha o hasp como isto:



“Vire o disco duas plenas rotações da esquerda para a direita ao primeiro número da combinação. Então vire-o ao contrário dos ponteiros do relógio passando o primeiro número ao segundo número. Então vire o disco da esquerda para a direita ao terceiro número e o cadeado abrirá.”

Você agora pode ver por que você tem que fazer isso. O desvio o disco 2 plenas revoluções recebe os dentes de todos os três cams empenhou, então o três cams viram em uníssono. Agora quando vira ao contrário dos ponteiros do relógio só o cam superior gira. Como vai passado o primeiro número, o primeiro cam dente empenha o segundo cam, tão agora o dois cams movem. A fricção fornecida pela mola, no entanto, mantêm o terceiro cam em sua posição. Quando vira o disco da esquerda para a direita outra vez, só o cam superior gira. Uma vez todas três entrâncias são alinhadas adequadamente por este processo, e o cadeado abre.

SEGUNDA PARTE DO CURSO

Abrir fechaduras com uma Bumping Key

Este artigo dirige-se não só aos amantes de *lockpicking*, mas sim ao publico em geral, uma vez que a grande maioria das fechaduras existentes em estão vulneráveis a este tipo de ataque.

Membros da [Toool](#) estiveram no [What The Hack](#) a apresentar um método relativamente recente que possibilita abrir fechaduras e cadeados topo de gama em poucos segundos, sem a utilização de um *lockping kit*. Apesar de partilharmos a informação da nossa experiência e utilização do método, não nos responsabilizamos por qualquer acção punível por lei que daqui possa surgir.

Apenas queremos alertar o publico em geral para estas questões de segurança física.

Seguem algumas fotos e texto adicional:

Basicamente a ideia é encontrar uma chave que consiga entrar na fechadura que queremos abrir (obviamente que não a abra, senão não era necessário mais nada;), alterá-la e depois abrir a fechadura em poucos segundos.

Vamos então meter mãos à obra com a seguinte lista de material:



Uma lima de arestas triangulares, uma fechadura de porta, uma chave que entre na fechadura e um pequeno torno (não incluído na foto).

Aparência da chave normal:



Passemos a construir a Bumping key:



Este processo chama-se construção de uma chave 999, ou seja, os Vértices inferiores são limados até abaixo de modo a ficarem todos iguais ao mesmo nível.

Bumping key já finalizada:



Podemos ver os vertices já limados e o batente da chave também retirado de modo a que a chave possa entrar um pouco mais na fechadura.

Aparência da chave normal e da bumping:



Podem ver a chave normal e a bumping key já terminada.

Vamos então testar a bumping key:



Para testar a bumping key, prendemos a fechadura firmemente no torno e inserimos a chave.

Com uma mão seguramos a chave entre o indicador e o polegar com a outra com o cabo da lima vamos dando umas pancadas:



ao mesmo tempo que tentamos rodar a chave:



Este processo baseia-se no mesmo princípio da física das pistolas de locking utilizadas por profissionais na área.

O processo de bater a chave para dentro da fechadura, gera forças que impulsionam os pinos para cima, possibilitando com alguma prática sincronizar os movimentos e conseguir muito facilmente rodar a chave em poucos segundos, equivalendo apenas a umas duas ou três pancadas.

Se não funcionar à primeira, nem à segunda, continuem até lhe apanhar o jeito, ou até os pinos moldarem a chave, uma vez que a liga metálica de que é feita a chave é mais mole que os a liga dos pinos.

Provavelmente muitos de vocês estão a pensar algo do tipo:

- Com tantas fechaduras diferentes, temos de andar com uma mochila cheia de chaves para conseguir encontrar uma que consiga entrar na fechadura que pretendemos.

Sim e não, ou seja, sim existem muitas fechaduras diferentes, mas se, por exemplo, forem a uma casa de chaves e perguntarem quantas chaves são encomendadas mensalmente, a resposta será por volta de uma centena de chaves diferentes.

No entanto, se perguntarmos de entre a centena de chaves quais as que são mais utilizadas em fechaduras e cadeados a resposta será apenas pouco mais do que uma dezena.

Esse grupo de dez chaves são precisamente as chaves mais comuns para as fechaduras e cadeados da zona.

Não custa nada alertar as pessoas para este tipo de ataque, pois é extremamente difícil uma seguradora cobrir o prejuízo de uma casa que foi assaltada, sem qualquer vestígio de entrada forçada.

Sim claro que estão a pensar que em uma situação dessas, o dono da casa pode ele próprio causar danos na fechadura para que a seguradora pague.

A realidade não é bem assim, pois a seguradora irá primeiro que tudo investigar que não foi o próprio dono a causar os danos, e acreditem que existem bons peritos.

LOCKPICKING

O lockpicking, é um conjunto de técnicas que permitem abrir uma fechadura quase sem deixar vestígios.

Existem vários sistemas de segurança, com princípios funcionamentos diferentes. Cada sistema terá uma abordagem diferente, e será mais ou menos vulnerável ao lockpicking.

O lockpicking pode ser utilizado para fins ilegais, mas é raro, porque a abordagem destrutiva é mais simples de dominar e mais rápida na maioria dos casos.

Uma aplicação mais lógica no domínio ilegal seria para a espionagem, mas os sistemas mais avançados são quase invulneráveis à este tipo de ataques, e necessitam instrumentos mais caros e mais difíceis encontrar, quando existem.

Mais uma vez a abordagem mais utilizada pelos espiões é destruir o sistema e substituí-lo por um que pode ser aberto por todas as chaves da mesma marca instalada. A pessoa chegará abrirá normalmente com a sua chave e não desconfiará de nada.

Então para que serve o lockpicking finalmente?

O lockpicking é antes um hobby, praticado por alguns profissionais das fechaduras e alguns amadores de fechaduras e de sistemas de fecho.

Algumas pessoas comparam o lockpicking a puzzles, o que é de uma certa maneira verdade, no que diz respeito as aberturas feitas com os picks.

Uma outra técnica muito interessante de um ponto de vista desportivo é a impressão.

O lockpicking é mais interessante se as fechaduras possuem sistemas anti lockpicking, abrir uma fechadura com racle também não é muito interessante.

Atenção

Certas pessoas são roubadas sem vestígios de arrombamento, as pessoas metem-se a crer no que vêem nos filmes, é muito raro que alguém utilize este tipo de técnicas.

Procure antes a sua volta, ou pessoas que puderam ter acesso à sua chave para fazer uma cópia, ou ainda se fecham a vossa porta à chave cada vez que sai, porque as portas batidas podem ser abertas com o by-pass.

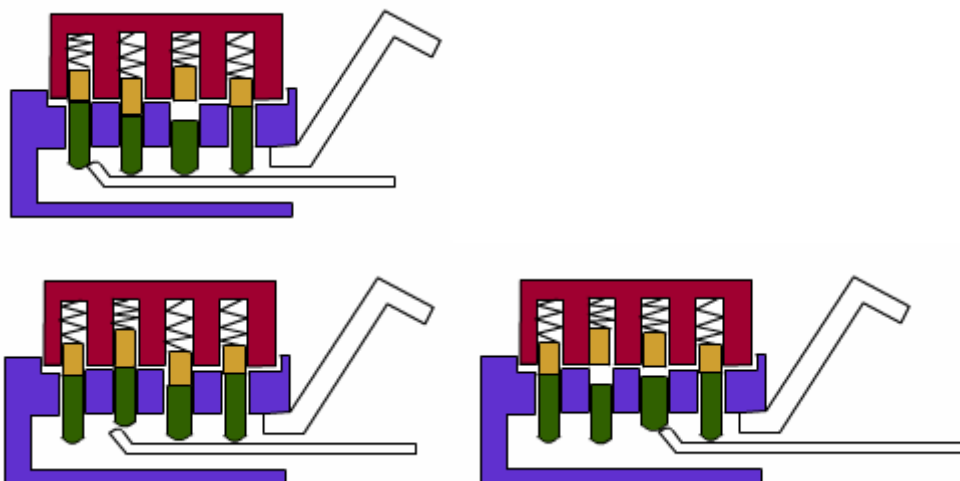
As fechaduras de segurança contrariamente ao que se pode crer são mais fáceis de abrir quando estão batidas, isto é devido a sistemas mais perfeitos que transformam o fecho mais fácil, mas atenção uma vez as portas fechadas à chave as fechaduras de elevada segurança asseguram uma resistência ao arrombamento muito elevada.

As técnicas como o pickgun ou as bumpkeys são técnicas destinadas a demonstrar falhas mais graves que possuem certos sistemas de segurança.

Os Picks

Com a ajuda dos picks metemos as golpilhas sobre a linha de interrupção uma a uma até à abertura da fechadura.

A figura abaixo permite de visualizar o que se passa dentro da fechadura.



As fechaduras com golpilhas únicas e não com pares de golpilhas, com quatro ou cinco unidades não oferecem uma boa resistência aos picks, encontra-se este tipo de fechaduras em algumas montras, caixas de correio, automóveis antigos, armários nos escritórios etc.. Por exemplo a minha abertura de porta mais rápida com os picks permanece e permanecerá muito tempo uma porta de um Mini antigo, precisei de menos de cinco segundos para abrir-o, então se tem um automóvel de colecção, um alarme é indispensável.

Existe dois grandes métodos para abrir as fechaduras com os picks.

Racle - representado na animação em cima, consiste a fazer várias passagens com o pick (normalmente o meio diamante) até à abertura da fechadura, para o fazer é necessário controlar a velocidade, a pressão sobre as gol pilhas e a tensão de rotação, as golpilhas anti lockpicking são muito eficazes contra esta técnica, o problema é que muitas fechaduras não tem nenhum.

Alinhar as golpilhas uma a uma- consiste a encontrar a golpilha que bloqueia mais, sobe-se a golpilha até sentir uma queda na resistência e passa-se seguinte, até abrir a fechadura. Esta técnica é muito mais difícil de realizar em relação ao racle, mas ela é inevitável para abrir certas fechaduras, com sistemas anti lockpicking.

Na foto temos os picks que estão num kit principiante



À esquerda temos dois picks

que servem para fazer passagens em racle sobre várias golpilhas ao mesmo tempo. Pode-se comparar estes dois picks aos picks gerados por computador

O terceiro é um extractor de chaves partidas, pode servir também para abrir cadeados muito pequenos.

O quarto é o gancho, certos estojos possuem vários ganchos de diferentes dimensões.

O quinto é a serpente, certos estojos possuem vários.

O sexto é um meio diamante.

Em baixo temos dois utensílios de tensão, estes servem para aplicar uma tensão que vai tornar a abertura possível, sem estes as golpilhas voltariam para sua posição inicial.

Existe utensílios de tensão circulares que têm a mesma função, mas em certos casos são mais úteis, falta de espaço para trabalhar (proximidade do muro) ou então de fechaduras tipo as dos automóveis, porque exercem a tensão sobre a parte superior e a parte inferior da entrada da chave, o que torna a tensão de rotação mais uniforme.

Picks creados pour computador.



Este tipo de picks, são em geral mais difíceis de encontrar na Internet, eles são cerca de 15 o que faz 15×2 e ainda $\times 2$ porque podemos virá-lo ao contrario para termos outras combinações, o que faz ao todo 60 combinações diferentes, aplicando o método racle, pode-se abrir quase todas as fechaduras paracêntricas (as chaves comuns) se eles entrarem claro e com um pouco de técnica. Este tipo de picks foi criado para contornar as golpilhas com formas anti lockpicking.

Este tipo de picks não precisa de um treino específico para a sua utilização, o que o torna pouco interessante para o amador de lockpicking, ela é mais interessante para os serralheiros que podem fazer calmamente e experimentar todas as combinações, senão correm o risco de ter de recomeçar.

ALGUNS VÍDEOS COM OS PICKS

VEJA OS VÍDEOS APÓS DESCOMPATAR O ARQUIVO VÍDEOS .ZIP



VIDEO - 01

Fechadura de caixa do correio.

Fechadura com golpillhas "unicas".

Sem sistema anti lockpicking



VIDEO - 02

Cadeado pequeno.

Três golpillhas sem sistema anti lockpicking



VIDEO - 03

Fechadura de persiana metálica.

Fechadura com três golpilhas.
Sem sistema anti lockpicking.
As ultimas versões desta fechadura tem contra golpilhas



VIDEO - 04

Fechadura dos correios e entrada de imóveis.

6 golpilhas.
Não tem sistema anti lockpicking .



VIDEO - 05

Cilindro de fechadura JPM CISA

5 golpilhas.

Sistema anti lockpicking diabolos.



VIDEO - 06

Fechadura de tampão de gasolina de carro

Fechadura com quatro golpilhas "únicas".

A Bricard supersureté.



Esta fechadura também pode ser aberta com os picks.

Ao lado a fechadura, multi- pontos. Pelo momento não tem vídeo para esta fechadura, preciso de muito tempo para abrir esta fechadura. Isto e devido ao facto que todos os quartos de volta as golpilhas voltam para a posição fechada, será necessário alinhar as golpilhas 7 vezes e abrir a maçaneta com uma técnica de by pass para abrir uma porta

equipada com esta fechadura e fechada com duas voltas, ou então 10 vezes para abrir as duas voltas e a maçaneta com os picks, o que é lento.



Esta fechadura é interessante a abrir com os picks dum ponto de vista desportivo.

A esquerda temos um grande plano da fechadura aberta com os picks

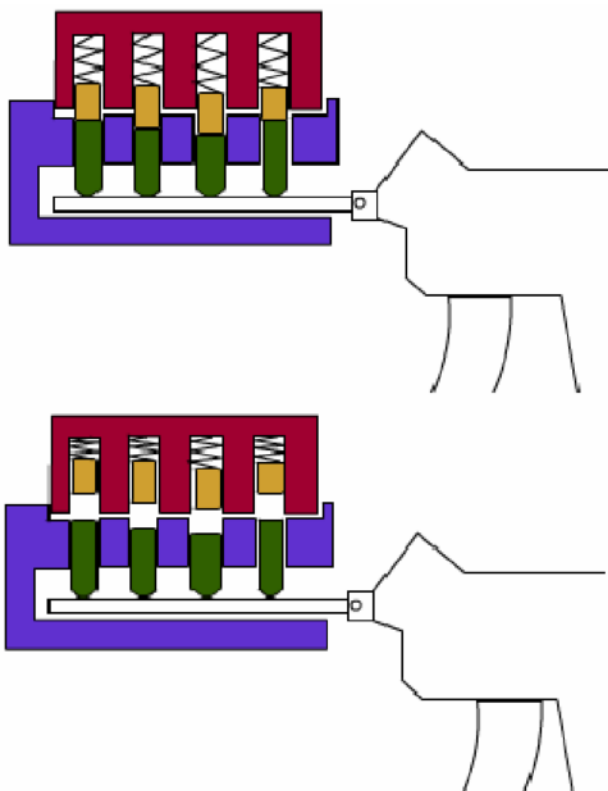


Chave Bricard supersureté.

PICK GUN

O pick gun é utilizado para criar um vazio entre as golpilhas ativas e as passivas e abrir facilmente fechaduras normais e algumas a micro pontos.

A figura abaixo permite de visualizar o que se passa dentro da fechadura.



Quando chamar um serralheiro para uma abertura de porta o Pick gun será talvez a única técnica de lockpicking que verá em ação. O Pick gun permanece a técnica mais fácil a dominar para efetuar uma abertura de porta, à condição que a fechadura possa ser aberta com esta técnica.

O funcionamento desta técnica.



A maneira mais simples de abrir as fechaduras que funcionam com pares de golpilhas é dar um golpe seco sobre as golpilhas, isto vai provocar uma transferência de energia entre a golpilha e contra golpilha, que vai fazer com que a golpilha permaneça em baixo e a contra golpilha suba sozinha, isto vai criar um vazio entre golpilha e contra golpilha que vai permitir abrir a fechadura durante algumas pequenas frações de segundo. Como ao bilhar, se tivermos duas bolas uma contra a outra, quando batemos na primeira bola esta vai transferir a energia recebida à segunda bola e é esta que vai deslocar-se enquanto a que recebeu o golpe inicialmente permanece no mesmo sitio ou quase.

O pick gun e as golpilhas anti lockpicking.

As golpilhas anti-lockpicking tornam o trabalho do Pick Gun mais complicado, mas a abertura continua a ser possível. Nos sistemas anti lockpicking as golpilhas passivas são mais eficazes que as golpilhas ativas em geral. O mais curioso é que os sistemas anticrochetage que funcionam melhor contra o Pick Gun são mais vulneráveis aos picks, e aquelas que são melhores contra picks são mais vulneráveis contra o Pick Gun.

O Bumping e o Pick Gun funcionam com o mesmo princípio, mas fora do laboratório o Pick gun talvez seja mais eficaz para uma abertura de porta que o bumping, porque sobre o terreno as fechaduras são a maior parte do tempo antigas, ligeiramente oxidadas ou sujas e o bumping tem algumas dificuldades nestas condições, ele funciona melhor sobre fechaduras novas ou quase novas.

Os vários Pick Gun.

Pick Gun manual.

Sobre os mais sofisticados, pode-se regular a potência dos golpes, o que permite de se adaptar às características de cada marca, e superar alguns sistemas anti lockpicking, escolher o sentido dos golpes para cima para as fechaduras normais, para baixo para as fechaduras de modelo europeu, com o clássico como aquele que está na foto temos de vira-lo ao contrário o que torna mais complicado dar bons golpes.

Pick gun feito em casa.

Estes utensílios são feitos apenas com um martelo, arame, lima e um alicate.



pick gun improvisado, mas não podemos comparar a eficácia dos outros pick gun com estes, mas é interessante de ver este pick gun em acção.

Pick gun Elétrico

Mais simples a utilizar, o princípio continua a ser o mesmo enquanto apoiar sobre o botão a lâmina vibra. Existe dois fabricações diferentes, certos modelos aproveitam a rotação de um motor para fazer vibrar a lamina, outros possuem uma bobine que vai atrair uma parte de metal que tem o gancho à extremidade, isto vai cortar o circuito, a bobine não é alimentada tudo volta a posição inicial isto fecha o circuito a bobine atrai a peça metálica que vai cortar o circuito e tudo recomeça.

Pickgun Elétrico feito em casa.

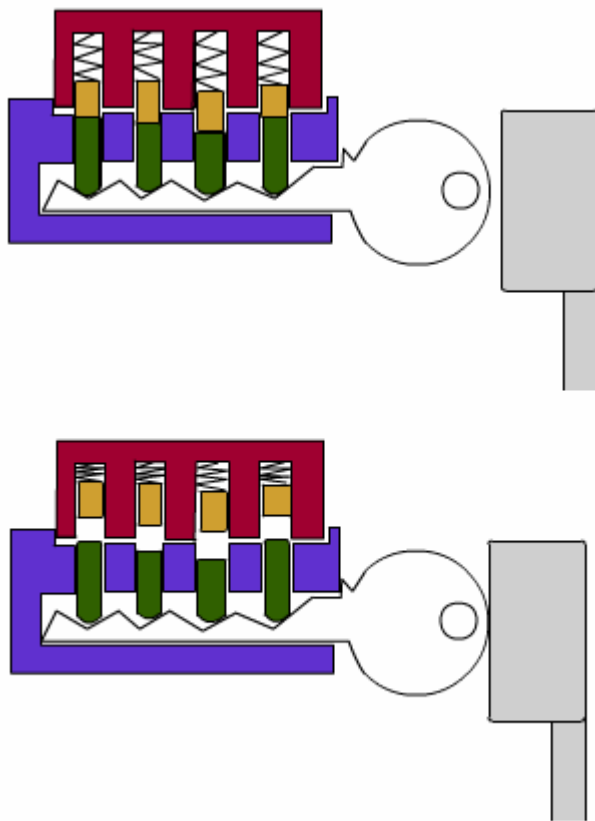
Podemos encontrar na Internet pick gun elétricos feitos a partir de escovas de

dentes elétricas, máquinas de aparafusar, máquinas de cortar cabelo HD de computador e com tudo que tem um motor.

O Bumping

O Bumping serve a criar um vazio entre as golpilhas e contra-golpilhas e abrir facilmente fechaduras paracêntricas e certas fechaduras de uma segurança elevada.

A figura abaixo permite de visualizar o que se passa dentro da fechadura.



A maneira mais simples de abrir as fechaduras que funcionam com pares de golpilhas é dar um golpe seco sobre as golpilhas, isto vai provocar uma transferência de energia entre a golpilha e contra golpilha, que vai fazer com que a golpilha permaneça em baixo e a contra golpilha suba sozinha, isto vai

criar um vazio entre golpilha e contra golpilha que vai permitir abrir a fechadura durante algumas pequenas frações de segundo. Como ao bilhar, se tivermos duas bolas uma contra a outra, quando batemos na primeira bola esta vai transferir a energia recebida à segunda bola e é esta que vai deslocar-se enquanto a que recebeu o golpe inicialmente permanece no mesmo sitio ou quase.

O bumping e as aberturas de porta.

Se chamar um serralheiro para uma abertura de porta, dificilmente ele o fara com o bumping, porque não se consegue comprar as bump keys nos fornecedores habituais.

O que é uma Bump key



Uma Bump key é uma chave feita a partir de uma chave 999, ou de uma depth key, termos técnicos para dizer uma chave da marca com todos os cortes ou buracos à profundidade máxima utilizado sobre as chaves desta marca. Uma chave 999 vai abrir muitas fechaduras desta marca mas para abrir um maior número, os fabricantes aumentam mais pouco a profundidade dos buracos ou dos cortes e limam um bocado o batente e às vezes a extremidade da chave para permitir à chave de entrar mais um bocado na fechadura para criar um desnível sobre as golpilhas.



Em cima as bumpkeys, todas feitas com uma lima e abriram pelo menos uma fechadura.

Ao lado uma Bumpkey de uma fechadura a micro pontos , feita com uma máquina de copiar chaves. Como pode-se ver o primeiro e o último buraco são bastante profundos, o que não impediu a fechadura de ser aberta.



Sobre esta fotografia tem-se a bumpkey e a chave, pode-se ver que apesar da diferença a fechadura é aberta facilmente.

O bumping

Método antigo.

O método antigo consiste em entrar a Bump key puxar um corte e bater sobre a chave e rodar um bocadinho depois de bater ou então quando se bate aplicasse uma força de rotação muito ligeira. A tensão de rotação é fácil de dominar sobre uma fechadura que não tem golpilhas anti lockpicking, mas para as outras muitas vezes é necessário um timing muito preciso para abrir a fechadura, é necessário bater e imediatamente depois rodar a bumpkey.

Método do movimento mínimo

Quando metemos a bumpkey na fechadura esta sai ligeiramente, porque quando se limou criou-se uma desfasamento entre os cortes e as golpilhas, ao deixar a chave como as golpilhas se encontram na inclinação as molas vão empurrar as golpilhas contra a chave e como estas se encontram na inclinação ela sai para fora até ficar entre as duas inclinações, vamos chamar a isto "posição de repouso". Para abrir a fechadura com este método metemos a bump key na posição de repouso, mandamos uma pancada na bump key com o instrumento da nossa escolha e aplicamos o método de rotação descrito em cima.

O falso bumping "bumping low impact"

Esta técnica consiste em meter e tirar a bumpkey e rodar ao mesmo tempo até a abertura da fechadura, isto não funciona como o bumping mas mais como a abertura com passagens sucessivas dos picks (ver a pagina picks), é preciso dizer também que esta técnica funciona sobre um número muito limitado de fechaduras da marca em questão. É absurdo comparar esta técnica com o bumping porque o princípio não é o mesmo, e como técnica de lockpicking não é muito eficaz, ela abre apenas certas combinações e à condição que as golpilhas se alinhem numa ordem específica. Não posso dizer a percentagem de fechaduras que podem ser abertas assim mas é muito muito baixo. Em contrapartida esta técnica é muito útil com as chaves traficadas.

Algumas verdades sobre o bumping.

Este método de abertura fez muito barulho na Alemanha e nos países nórdicos, e é quase desconhecido no resto da Europa.

O bumping funciona melhor sobre fechaduras novas que sobre fechaduras que já tenham servido alguns anos, a oxidação e a sujeira que acaba por entrar na fechadura vai "bloquear as contra-golpilhás" estas poderão não subir o necessário para permitir a abertura.

Nas fechaduras antigas o Pick Gun é mais eficaz em geral.

O bumping precisa de uma chave diferente para cada marca e cada modelo terá um bumpkey diferente.

Para as chaves "normais" dos cilindros paracêntricos sobre um catálogo temos mais de um milhar de bumpkeys a fazer, mas há uma dezena de bumpkeys que vai abrir mais de metade das fechaduras no mercado. Isto é verdade para a maior parte dos países, uma dezena de chaves abre mais da metade das fechaduras, mas as dez alemãs não são as mesmas que as 10 francesas, com um pouco de sorte há duas ou três que coincidem, mas nenhuma no topo da lista.

Um detalhe importante são as chaves "universais" que permitem fazer vários modelos, mas as bump keys feitas nos passes são mais frágeis, e certas marcas tem as golpilhás em posições diferentes o que vai tornar a abertura aleatória.

Para as chaves de segurança e segurança elevada a coisa é mais delicada, certas marcas podem ser abertas muito dificilmente e outras facilmente mas certas pessoas tem tendência a por tudo no mesmo cesto.

Se pudéssemos simplificar diria que para as chaves com micro pontos, seis buracos de cada lado da chave e sem buracos laterais são mais ou menos fáceis de abrir a partir de 10 buracos será difícil de abrir. Um meio para saber quantos pares de golpilhás tem a fechadura é contar todos os buracos presentes na chave e dividir por dois. Apenas algumas fechaduras tem golpilhás em todos os buracos.

O problema com o bumping é que aquele que quer desmontar o bumping vai procurar uma fechadura no seu stock que abre facilmente e vai mostrar que o bumping a abre e esquece todas aquelas que ele não abre, os fabricantes fazem o contrário.

Pode-se encontrar na internet listas com fechaduras abertas com o bumping mas as mais viáveis estão no site de toool, e algumas fechaduras que estão presentes mostram que elas são vulneráveis ao bumping e não que não importa quem pode ter uma bump key para o fazer, e que funciona sobre todas as fechaduras.

Mas é importante dizer que até à seis pares de golpilhás, as fechaduras serão vulneráveis à este tipo de abertura.

As Bumpkeys para as fechaduras paracêntricas e para certas fechaduras cruciformes podem ser feitas á mão com uma chave da marca e uma lima. As Bumpkeys para as fechaduras a micro pontos necessitam de uma maquina para copiar chaves a micro pontos e muita técnica, ou então uma máquina de reprodução de chaves com código e pouca técnica.

Fechaduras de Código



A maior parte dos cadeados de combinação abre-se seguindo o método seguinte:

forçamos a asa ou botão no sentido da abertura, gira-se as rodas de combinação e frequentemente sente-se uma diferença com ao tocar ou um clique diferente, quando passa sobre a boa combinação. Não devemos esquecer que a diferença é muito pequena e é necessário estudar o barulho, a maneira que a roda com os números desliza entre as posições se há uma reação mesma que muito pequena sobre a asa. Os cadeados de metal no gênero daquele que esta na fotografia, abrem-se facilmente empregando o método descrito em cima, mas os que está sobre a fotografia é mais difícil de abrir por este método, porque as rodas são de plástico e amortecem as diferenças que existem durante a passagem pela boa posição.



Em contrapartida o fato que sejam de plástico permite deslizar um pick e sentir diretamente os buracos que vão permitir abrir o cadeado. Certamente que certos cadeados possuem de sistemas anti lockpicking com cortes falsos que tornam a abertura ainda mais complicada, as vezes é impossível ou quase de achar a boa combinação diretamente, mas podemos ao menos diminuir consideravelmente o numero de combinações possíveis.



Certos cadeados como este ao lado possuem um meio original para esconder as diferenças, possuem uma lingueta que vai parar os números perfeitamente em cada numero, o problema é que ela cria cliques que vão esconder as diferenças ao tocar e de som, e temos dificuldade a encontrar a combinação, a solução consiste em pôr bocadinhos de metal muito finos que vão anular a ação da lingueta, e agora sim podemos encontrar a combinação aplicando o método das sensações. Para tentar uma combinação é necessário retirar a folha

metálica porque as combinações são muito precisas.
Existe também o mesmo tipo de aloquetes mas com falsas combinações. Que tornam isto tudo quase impossível, mas podemos ainda aqui diminuir o número de combinações possíveis.



As falsas combinações sobre o cadeado que tenho permitem de fazer uma leitura das combinações possíveis.

Procedemos com a técnica descrita em cima e vamos nos aperceber que cada roda poderá assumir valores pares ou ímpares o que nos faz para cada roda 5 combinações possíveis em vez de 10.

Visto assim não parece um grande avanço, mas se fazemos as contas vamos ver que já é um começo.

O meu cadeado que tem falsas entradas é um de 1000 combinações ou seja três rodas.

$$10 \times 10 \times 10 = 1000$$

Com o método da eliminação passamos a

$$5 \times 5 \times 5 = 125$$

o que é oito vezes menos combinações.

Para um com quatro rodas como o da fotografia e com falsas entradas temos 625 contra 10 000 o que faz 16 vezes menos.

Sobre o meu aloquete de três números consegui encontrar a boa combinação ao fim de 30 ensaios.

Aqui vamos misturar as duas técnicas para contornar isto tudo, começamos com as 2 rodas que bloqueiam mais quando se puxa pela a asa, o que nos faz 25 (5*5) combinações a experimentar olha-se muito bem e as vezes pode se observar observar que a asa avança um bocadinho mais, isto quer dois bons

números depois você passa à terceira roda. Atenção a diferença é realmente pequena.

Claro que os fabricantes não param de melhorar os sistemas e os modelos topo de gama são quase impossíveis de ir mais longe que diminuir as combinações possíveis.



Este tipo de cadeados, é invulnerável a este tipo de manipulações, mas podemos os abrir com uma tecnica de by pass os shims.

Podemos também encontrar sites descrevendo como os abrir, mas isto funciona apenas sobre os antigos.

Uma das coisas que se pode fazer é diminuir consideravelmente o número de combinações possíveis por puxando a asa e passa-se: $40 \times 40 \times 40$, ou seja, 64.000 combinações $12 \times 12 \times 11$ seja 1584 combinações.

Vi uma vez na Internet um pequeno aparelho que se aplica-se sobre a roda da combinação, e o aparelho faz a rodar muito rapidamente e tenta todas as combinações em 30 minutos, "ao que parece".

FIM