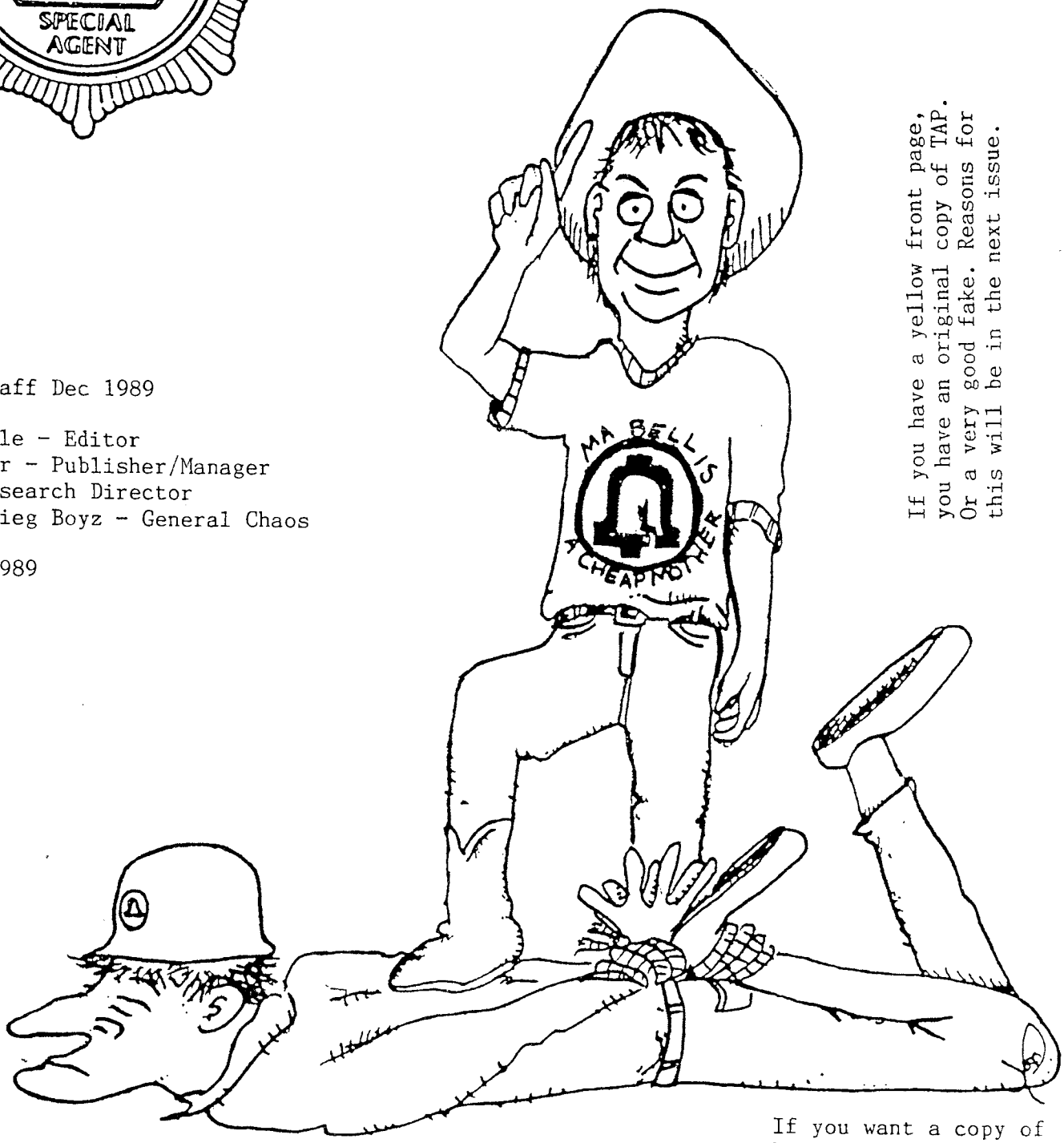
TAP ISSUE #96
12-25-1989
Lockpicking Special Edition

Happy New Year
The Neoteric Strain Of
Phreakers For The 90's

TAP
P.O. Box 20264
Louisville, Ky 40220



If you have a yellow front page, you have an original copy of TAP. Or a very good fake. Reasons for this will be in the next issue.

TAP Staff Dec 1989

Aristotle - Editor
PredatOr - Publisher/Manager
Ed - Research Director
Blitzkrieg Boyz - General Chaos

12-25-1989

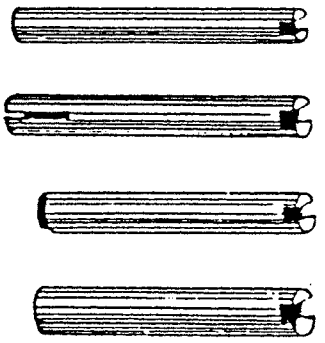
If you want a copy of this issue please send us 2 quarters or a .50¢ piece. No Checks Please

Lock-Pick Larceny
By
Alexander Mundy

I hope all of you TAP readers have either made or acquired your lock picks, because I will teach you how to use them.

In order to get started, you will need the following equipment:

1. A pair of tweezers
2. A set of followers



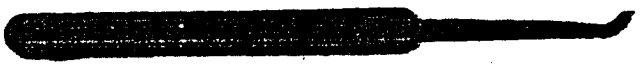
Picture from HPC catalogue

You TAP readers can make a set of followers from brass or plastic round stock or tubing. The important point to remember, is in making the follower, the end must match the plug. When you push the follower through the shell, the top pins and springs should not fall down in between the plug and follower.

3. Rim or Mortice cylinders (stay away from the ones with a curved keyway, like Yale and Lockwood and also the ones with mushroom or spool pins, like Corbin and Russwin.)

These cylinders are harder to pick for the average beginner.

In order to start, remove the tail piece of the cylinder. It is usually held on by two screws or a spring clip. Next, take a follower and remove the plug from the shell. Be careful not to drop any of the pins. Also, when pushing the plug out of the shell, make sure that the key is slightly turned and that the follower is firmly against the plug. Otherwise, you will jam one of the top pins or springs between the plug and the follwe as you are pushing out the plug.



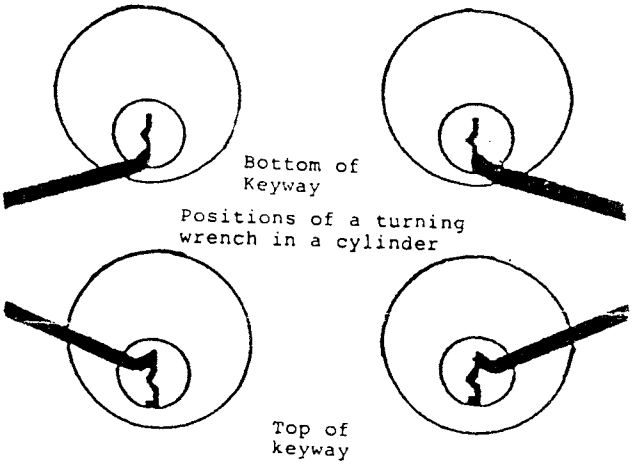
Next, remove all the bottom pins, except one. It's position in the plug does not matter. Also, remove all the top pins and springs, except the one that matches the bottom pin. Now reassemble the plug in the shell. Be Careful that the top pin and spring does not fall into any of the unused pin chambers in the plug. Take your turning wrench and pick (you should use a hook pick like this)

Insert your wrench into the cylinder and exert pressure on the plug via the wrench. Next, take your pick and puch up the one pin so that it reaches the shrear line. The plug will turn in the shell. Congratulations!!! You have just picked a one pin cylinder.

For your next experiment, try putting different amounts of pressure onthe wrench and feel the difference as you push up the pin. Also, use your wrench in the various positions shown. After you get the feel of picking the one pin, try moving that pin to a different pin chamber. Don't forget about the top pin and spring.

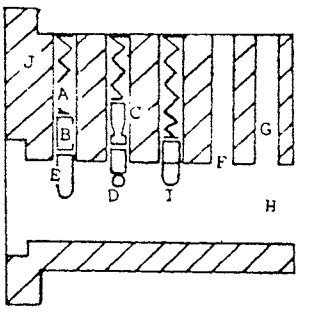
After practicing for awhile, try adding another top and bottom pin and spring to the cylinder and practive some more. Keep picking and also remember the feel you are acquiring. Soon you will be able to work your way up to 5, 6, and 7 pin cylinders.

P.S. While picking a cylinder, you should keep the cylinder steady by placing it in a vice or other suitable holder.



Positions of a turning wrench in a cylinder

Pressure may be applied wither upward or downward on the turning wrench.



A. Cylinder Spring
B. Top Pin
C. Mushroom Top Pin
D. Ball Bearing and Top Pin used as a Bottom Pin
E. Regular Bottom Pin
F. Shear Line
G. Pin Chamber
H. Plug (the part where the key fits in)
I. Top and Bottom Pin at the Shear Line
J. Shell

The shell and the plug along with the springs, top pins and bottom pins, forms a cylinder.

Continued From Issue #95

I. Tools

This section describes the design and construction of lock picking tools

I.1 Pick Shapes

Picks come in several shapes and sizes. Figure I-1 shows the most common shapes. The handle and tang of a pick are the same for all picks. The handle must be comfortable and the tang must be thin enough to avoid bumping pins unnecessarily. If the tang is too thin, then it will act like a spring and you will loose the feel of the tip interacting with the pins. The shape of the tip determines how easily the pick passes over the pins and what kind of feedback you get from each pin.

The design of a tip is a compromise between ease of insertion, ease of withdrawal and feel of the interaction. The half diamond tip with shallow angles is easy to insert and remove, so you can apply pressure when the pick is moving in either direction. It can quickly pick a lock that has little variation in the lengths of the key pins. If the lock requires a key that has a deep cut between two shallow cuts, the pick may not be able to push the middle pin down far enough. The half diamond pick with steep angles could deal with such a lock, and in general steep angles give you better feedback about the pins. Unfortunately, the steep angles make it harder to move the pick in the lock. A tip that has a shallow front angle and a steep back angle works well for Yale locks.

The half round tip works well in disk tumbler locks. See section 9.13. The full diamond and full round tips are useful for locks that have pins at the top and bottom of the keyway.

The rake tip is designed for picking pins one by one. It can also be used to rake over the pins, but the pressure can only be applied as the pick is withdrawn. The rake tip allows you to carefully feel each pin and apply varying amounts of pressure. Some rake tips are flat or dented on the top to make it easier to align the pick on the pin. The primary benefit of picking pins one at a time is that you avoid scratching the pins. Scrubbing scratches the tips of the pins and the keyway, and it spreads metal dust throughout the lock. If you want to avoid leaving traces, you must avoid scrubbing.

The snake tip can be used for scrubbing or picking. When scrubbing, the multiple bumps generate more action than a regular pick. The snake tip is particularly good at opening five pin bounebold locks. When a snake tip is used for picking, it can set two or three pins at once. Basically, the snake pick acts like a segment of a key which can be adjusted by lifting and lowering the tip, by tilting it back and forth, and by using either to top or bottom of the tip. You should use moderate to heavy torque with a snake pick to allow several pins to bind at the same time. This style of picking is faster than using a rake and it leaves as little evidence.

I.2 Street cleaner bristles

The spring steel bristles used on street cleaners make excellent tools for lock picking. The bristles have the right thickness and width, and they are easy to grind into the desired shape. The resulting tools are springy and strong. Section I.3 describes how to make tools that are less springy.

The first step in making tools is to sand off any rust on the bristles. Course grit sand paper works fine as does a steel wool cleaning pad (not copper wool). If the edges or tip of the bristle are worn down, use a file to make them square.

A torque wrench has a head and a handle as shown in figure I-2. The head is usually 1/2 to 3/4 of an inch long and the handle varies from 3 to 4 inches long. The head and the handle are separated by a bend that is about 80 degrees. The head must be long enough to reach over any protrusions (such as a grip-proof collar) and firmly engage the plug. A long handle allows delicate control over the torque, but if it is too long, it will bump against the doorframe. The handle, head and bend angle can be made quite small if you want to make tools that are easy to conceal (e.g., in a pen, flashlight, or belt buckle). Some torque wrenches have a 90 degree twist in the handle. The twist makes it easy to control the torque by controlling how far the handle has been deflected from its rest position. The handle acts as a spring which sets the torque. The disadvantage of this method of setting the torque is that you get less feedback about the rotation of the plug. To pick difficult locks you will need to learn how to apply a steady torque via a stiff handled torque wrench.

The width of the head of a torque wrench determines how well it will fit the keyway. Locks with narrow keyways (e.g., desk locks) need torque wrenches with narrow heads. Before bending the bristle, file the head to the desired width. A general purpose wrench can be made by narrowing the tip (about 1/4 inch) of the head. The tip fits small keyways while the rest of the head is wide enough to grab a normal keyway.

The hard part of making a torque wrench is bending the bristle without cracking it. To make the 90 degree handle twist, clamp the head of the bristle (about one inch) in a vise and use pliers to grasp the bristle about 3/8 of an inch above the vise. You can use another pair of pliers instead of a vise. Apply a 45 degree twist. Try to keep the axis of the twist lined up with the axis of the bristle. Now move the pliers back another 3/8 inch and apply the remaining 45 degrees. You will need to twist the bristle more than 90 degrees in order to set a permanent 90 degree twist.

To make the 80 degree head bend, lift the bristle out of the vise by about 1/4 inch (so 3/4 inch is still in the vise). Place the shank of a screw driver against the bristle and bend the spring steel around it about 90 degrees. This should set a permanent 80 degree bend in the metal. Try to keep the axis of the bend perpendicular to the handle. The screwdriver shank ensures that the radius of curvature will not be too small. Any rounded object will work (e.g., drill bit, needle nose pliers, or a pen cap). If you have trouble with this method, try grasping the bristle with two pliers separated by about 1/2 inch and bend. This method produces a gentle curve that won't break the bristle.

A grinding wheel will greatly speed the job of making a pick. It takes a bit of practice to learn how make smooth cuts with a grinding wheel, but it takes less time to practice and make two or three picks than it does to hand file a single pick. The first step is to cut the front angle of the pick. Use the front of the wheel to do this. Hold the bristle at 45 degrees to the wheel and move the bristle side to side as you grind away the metal. Grind slowly to avoid overheating the metal, which makes it brittle. If the metal changes color (to dark blue), you have overheated it, and you should grind away the colored portion. Next, cut the back angle of the tip using the corner of the wheel. Usually one corner is sharper than the other, and you should use that one. Hold the pick at the desired angle and slowly push it into the corner of the wheel. The side of the stone should cut the back angle. Be sure that the tip of the pick is supported. If the grinding wheel stage is not close enough to the wheel to support the tip, use needle nose pliers to hold the tip. The cut should should pass though about 2/3 of the width of the bristle. If the tip came out well, continue. Otherwise break it off and try again. You can break the bristle by clamping it into a vise and bending it sharply.

The corner of the wheel is also used to grind the tang of the pick. Put a scratch mark to indicate how far back the tang should go. The tang should be long enough to allow the tip to pass over the back pin of a seven pin lock. Cut the tang by making several smooth passes over the corner. Each pass starts at the tip and moves to the scratch mark. Try to remove less than a 1/16th of an inch of metal with each pass. I use two fingers to hold the bristle on the stage at the proper angle while my other hand pushes the handle of the pick to move the tang along the corner. Use whatever technique works best for you.

Use a hand file to finish the pick. It should feel smooth if you run a finger nail over it. Any roughness will add noise to the feedback you want to get from the lock.

The outer sheath of phone cable can be used as a handle for the pick. Remove three or four of the wires from a length of cable and push it over the pick. If the sheath won't stay in place, you can put some epoxy on the handle before pushing the sheath over it.

I.3 Bicycle spokes

An alternative to making tools out of street cleaner bristles is to make them out of nails and bicycle spokes. These materials are easily accessible and when they are heat treated, they will be stronger than tools made from bristles.

A strong torque wrench can be constructed from an 8-penny nail (about .1 inch diameter). First heat up the point with a propane torch until it glows red, slowly remove it from the flame, and let it air cool, this softens it. The burner of a gas stove can be used instead of a torch. Grind it down into the shape of a skinny screwdriver blade and bend it to about 80 degrees. The bend should be less than a right angle because some lock faces are recessed behind a plate (called an escutcheon) and you want the head of the wrench to be able to reach about half an inch into the plug. Temper (harden) the torque wrench by heating to bright orange and dunking it into ice water. You will wind up with a virtually indestructible heat screwdriver that will last for years under brutal use.

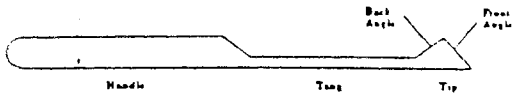
Bicycle spokes make excellent picks. Bend one to the shape you want and file the sides of the business end flat such that it's strong in the vertical and flexy in the horizontal direction. Try a right-angle hunk about an inch long for a handle. For smaller picks, which you need for those really tiny keyways, find any large-diameter spring and unbend it. If you're careful you don't have to play any metallurgical games.

I.4 Brick Strap

For perfectly serviceable key blanks that you can't otherwise find at the store, use the metal strap they wrap around bricks for shipping. It's wonderfully handy stuff for just about anything you want to manufacture. To get around side wards in the keyway, you can bend the strap lengthwise by clamping it in a vice and tapping on the protruding part to bend the piece to the required angle.

Brick strap is very hard. It can ruin a grinding wheel or key cutting machine. A hand file is the recommended tool for milling brick strap.

Diagrams next page.



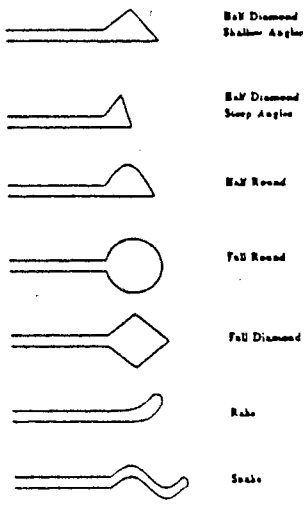


Figure I-1: Pick shapes

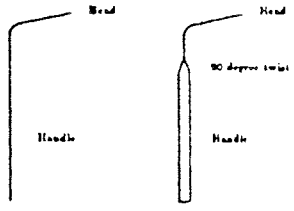


Figure I-2: Side view of tension wrenches

II. Legal Issues

Contrary to widespread myth, it is not a felony to possess lockpicks. Each state has its own laws with respect to such burglarious instruments. Here is the Massachusetts version quoted in entirety from the massachusetts general code

Chapter 266 (crimes against property)
Section 49 Burglarious instruments, making, possession, use

Whoever makes or mends, or begins to make or mend, or knowingly has in his possession, an engine, machine, tool or implement adapted and designed for cutting through, forcing or breaking open a building, room, vault, safe or other depository, IN ORDER TO STEAL THEREFROM money or other property, or to commit any other crime, knowing the same to be adapted and designed for the purpose aforesaid WITH INTENT TO USE OR EMPLOY OR ALLOW the same to be used or employed for such purpose, or whoever knowingly has in his possession a master key designed to fit more than one motor vehicle WITH INTENT TO USE OR EMPLOY THE SAME to steal a motor vehicle or other property therefrom, shall be punished by imprisonment in the state prison for not more than ten years or by a fine of not more than one thousand dollars and imprisonment in jail for not more than two and one half years

Emphasis added

In other words mere possession means nothing. If they stop you for speeding or something, and find a pick set, they can't do much. On the other hand, if they catch you picking the lock on a Monet machine they get to draw and quarter you.

States with similar wording include ME, NH, NY. One place that DOES NOT have similar wording and does make possession illegal, is Washington, DC. These are the only other places I have checked. I would imagine that most states are similar to Massachusetts but I would not bet anything substantial (say, more than a slice of pizza) on it.

It may be a good idea to carry around a xeroxed copy of the appropriate page from your state's criminal code.

End Of MIT Lockpicking Guide.

Picking Mushrooms

By Al Mundy (TAP

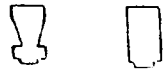
In this article, I will attempt to bestow upon the reader an additional piece of infinitesimal wisdom in the realm of technological knowledge. I trust all of you TAP readers have been practicing your lock picking, because I will dis close in this article the method of picking a cylinder (lock) with mushroom drivers. A mushroom driver looks like the following, also illustrated is a spool driver. Both of these top pins preform the same function.

Mushroom Driver Spool Driver

Corbin, Russwin, Abus, Walsaco, and American are some of the locks that contain mushroom pins. The Fox Police Lock Co. also uses a Russwin rim cylinder in its' lock products.

Now on to the technique. When one is confronted with a lock of this nature, one should pick the lock by first finding the bottom pin with the regular driver. There is usually only one regular top pin in a lock that contains mushroom drivers. But, the possibility exists that there may be more than one regular driver. While applying tension on the tension wrench, one picks the pins in the lock until one picks the one bottom pin with the regular driver. When the bottom pin with the regular driver reaches the shear line in the lock, the plug will turn a fraction of a degree. At this point, one know that you will have to pick the remaining bottom pins with the mushroom drivers. To push the bottom pin up to the shear line, one will have t gradually release tension on the tension wrench as you are pushing up on the bottom pin. As you are pushing up on the bottom pin, you will feel the plug begin to lose that fraction of a degree to which the plug was turned. When the bottom pin has reached the shear line, the plug will again turn a fraction of a degree. This will continue until all of the mushroom pins have been picked. At this time, the plug will be free to turn in the direction in which you have applied tension via the wrench.

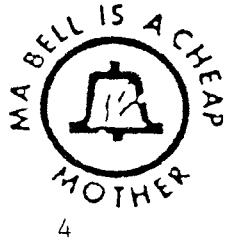
One exception to this is two types of fairly new drivers which loos as follows:



One should note the bottom lip of the pins

One would pick these in the same manner. But, before the lock will open, one will have to release almost all tension on the wrench. This is because the bottom lip of the top pin is still in the plug preventing the lock from opening. While having almost no tension on the wrench,. one will have to pick each bottom pin just a fraction more in order for the bottom pins to reach the sheer line.

GOOD LUCK AND KEEP ON TRYING!!!!!!!!!!!!!!!!!!!!!!



Many of the combination locks on the market today can be opened with a simple tool made from a piece of .005" spring steel that is gotten from an automotive feeler guage.

Any lock that has multiple combination wheels is openable by their method. The most notable brand is the Sesames combination lock.

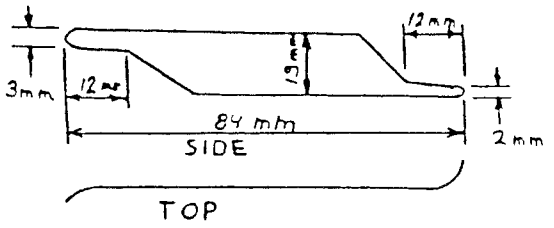
To make the pick out a piece of .005" steel to fit the pattern shown.

The steel should be heat treated a bit to the brittle side so that the feelers will not become flat during use.

To use insert the feeler between the combination wheel and the lock wall and turn the wheel until you find a notch in the side of the wheel. Do this to all the wheels. Now subtract or add 5 to the numbers you got. Now turn the wheels so that the resulting numbers face the trademark logo on the front of the lock.

This method can be varied to open most multi-wheel combination locks.

The Stainless Steal Rat

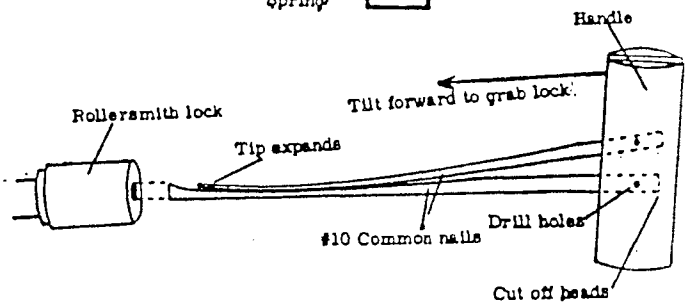


MAKE A KEY FOR YOUR ROLLERSMITH LOCK

One of our master craftspersons just built this beautiful rollersmith key and it works like a dream. Unlike the nail method in TAP 23, this key allows you to put the lock back on! (As well as take it off, of course). You'll need an ele-ctric grinding wheel and two 5/32" diameter nails. . . that are at least 3" long. Since the hole when the top nail is slid forward as shown in the diagram. Bend the backs of the nails so that there's a 1/8" space between them yet they lie flat against each other along their length. It's easy to see that when you tilt the handle forward the tip of the key expands and grabs the moving cylinder in the lock. Now pull the key outwards while keeping the top of the handle tilted forward, and voila! off it comes.

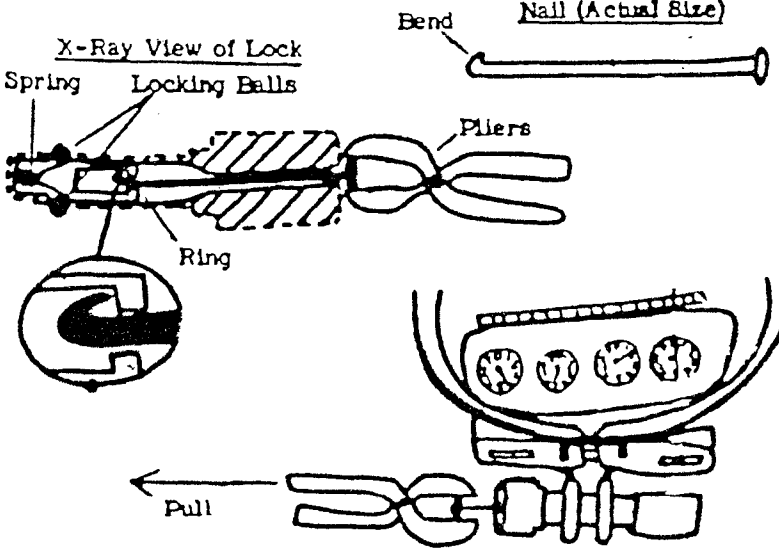
Drill the holes in the nails for the pivet screw and mount it in between two pieces of wood for a handle. You can put a rubber band around them so they don't flop around when not in use.

We smashed open a lock to find that it is built a little differently then we pictured in Issue 23. The spring is in the middle and there's no lip for a nail to grab.

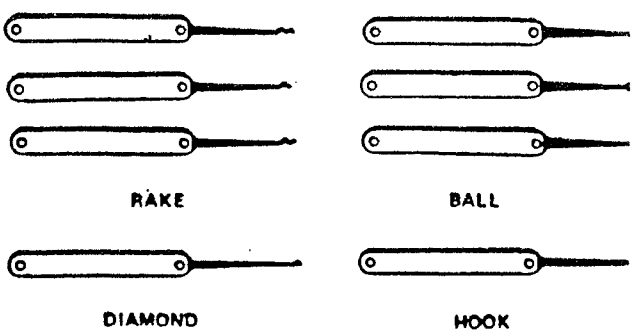


PICKING THE LOCK

To make a key for a rollersmith lock, take a 2" nail, size 8D or slightly larger, and bend up the tip a little as shown. You may have to tap it with a hammer to insert it a full inch and an eighth. Then use the bent tip to hook one of the rings inside. Pull the nail out very slowly and powerfully with a big pliers or visegrips. The spring in the lock is very hard and it will slip out a few times before you get it, but when it does the lock will open up. If you can't get it, just get a hacksaw and cut the ring.

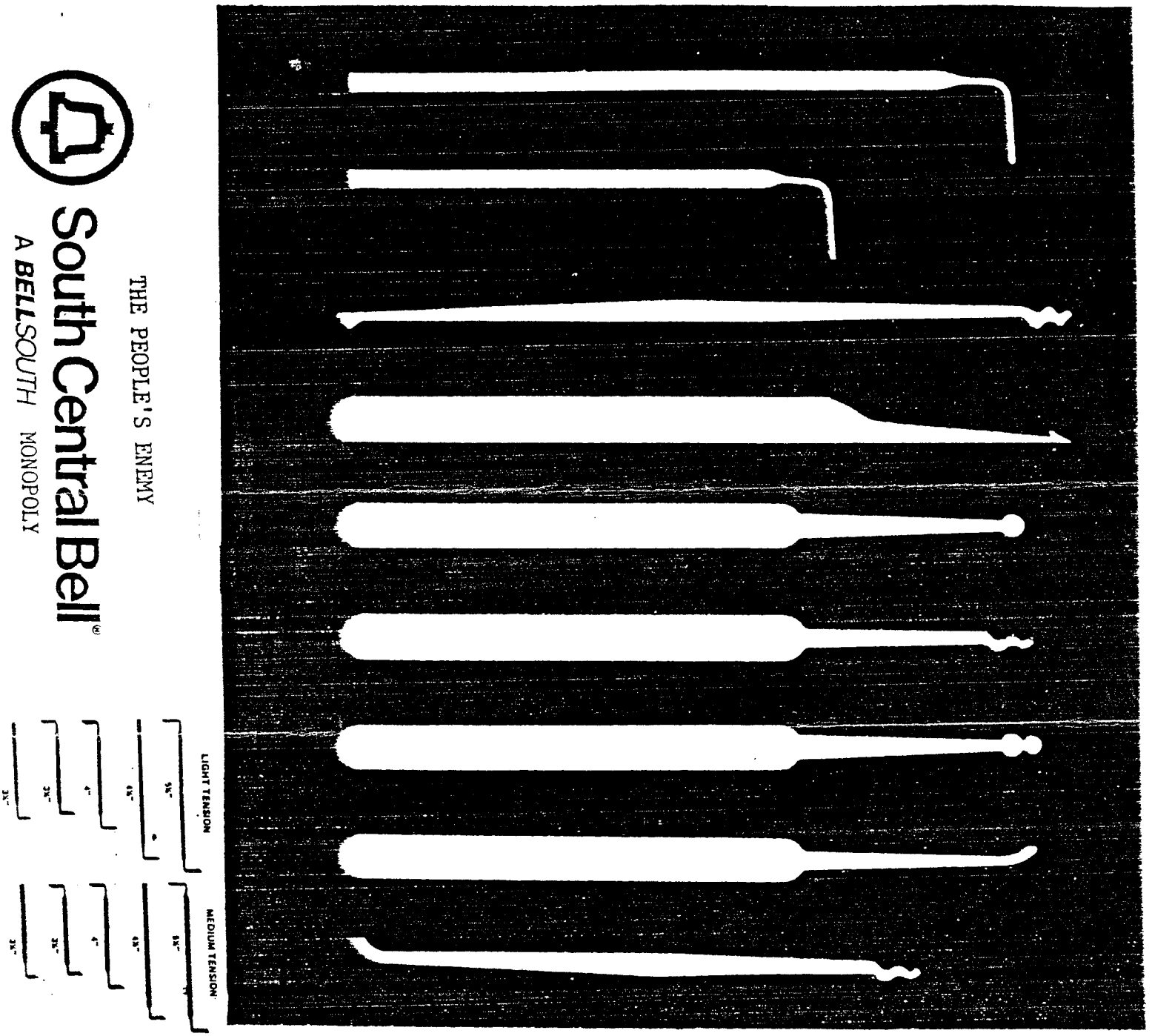


PICKING TOOLS



All picks shown are reduced from actual size.

PICK SET



Actual size/shape of a small, but adequate, pick set.

Subscriptions

All issues of TAP are free. (92 to current) To get issues you just need to send us a stamp, or a SASE to get a copy. We cannot give totally free subscriptions unless you are in jail. So when we run out of your stamps you are deleted from the mailing list. We will not send out a reminder. The last issue you will receive in on your mailing label. We provide the envelope, the paper, the time and effort and most important TAP itself, so please send us the stamps. 1 issue = 1 stamp. 10 stamps = 10 issues. SIMPLE? I know there are persons out there who can even send in a few extra stamps for the ones who cannot easily come by stamps. So donate a few to a fellow subscriber in need. Just tell us how many you want for your own greedy self and how many will go to others.