HOW TO BYPASS BIOS PASSWORDS

by Elf Qrin (http://www.ElfQrin.com)
v2.23 r03Sep2000-07Feb2001
First Release: r25Mar2000
The latest version of this document can be found at
http://www.ElfQrin.com/docs/biospw.html

The aim of this article is to explain how to break into a computer protected with a BIOS password. I'm not going to explain why you should do this. I assume it's your own computer and you forgot the password (however, by reading this article you should realize you can't rely on BIOS passwords if you need to secure your computer).
I hope you are not trying to crack a stolen laptop/notebook PC because I also own of them, and I wish you a hard disk crash with a complete loss of data you absolutely need in this case...

Accessing information on the hard disk

May be you don't actually need to access the computer, but you only need to access the information contained on the hard disk. In this case it could be more convenient to remove it temporarely from that machine and put it as a secondary hard disk on another machine, that you'll use as a host to retrieve data.
Before to put the hard disk on the host machine, set its jumper according to the EIDE channel to which you are connecting it (master, slave, or stand alone). Each disk drive has its own configuration, but it's usually explained on a sticker on the top. Take note of the original position of the jumper first, to set it back when you'll have to put the hard disk back to the original machine.
When you turn on the host machine, enter the CMOS setup menu (usually you have to press `F2`, or `DEL`, or `CTRL+ALT+S` during the boot sequence) and go to STANDARD CMOS SETUP, and set the channel to which you have put the hard disk as TYPE=Auto, MODE=AUTO, then SAVE & EXIT SETUP. Now you have access to the hard disk.

Standard BIOS backdoor passwords

The first, less invasive, attempt to bypass a BIOS password is to try on of these standard manufacturer's backdoor passwords:

AWARD BIOS

```
AWARD SW, AWARD_SW, Award SW, AWARD PW, _award, awkward, J64, j256,
j262, j332, j322, 01322222, 589589, 589721, 595595, 598598, HLT, SER,
SKY_FOX, aLLy, aLLY, Condo, CONCAT, TTPTHA, aPAf, HLT, KDD, ZBAAACA,
ZAAADA, ZJAAADC, djonet, %øåñòü ïpîáåëîâ%, %äåâÿòü ïpîáåëîâ%
```

AMI BIOS

```
AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, Oder
```

Other passwords you may try (for AMI/AWARD or other BIOSes)

```
LKWPETER, lkwpeter, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME,
Syxz, Wodj
```

Note that the key associated to "_" in the US keyboard corresponds to "`?`" in some European keyboards (such as Italian and German ones), so -- for example -- you should type `AWARD?SW` when using those keyboards. Also remember that passwords are Case

Sensitive. The last two passwords in the AWARD BIOS list are in Russian.

Flashing BIOS via software

If you have access to the computer when it's turned on, you could try one of those programs that remove the password from the BIOS, by invalidating its memory. However, it might happen you don't have one of those programs when you have access to the computer, so you'd better learn how to do manually what they do. You can reset the BIOS to its default values using the MS-DOS tool DEBUG (type DEBUG at the command prompt. You'd better do it in pure MS-DOS mode, not from a MS-DOS shell window in Windows). Once you are in the debug environment enter the following commands:

AMI/AWARD BIOS

```
O 70 17
O 71 17
Q
```

PHOENIX BIOS

```
O 70 FF
O 71 17
Q
```

GENERIC
Invalidates CMOS RAM.
Should work on all AT motherboards
(XT motherboards don't have CMOS)

```
O 70 2E
O 71 FF
Q
```

Note that the first letter is a "O" not the number "0". The numbers which follow are two bytes in hex format.

Flashing BIOS via hardware

If you can't access the computer when it's on, and the standard backdoor passwords didn't work, you'll have to flash the BIOS via hardware. Please read the important notes at the end of this section before to try any of these methods.

Using the jumpers

The canonical way to flash the BIOS via hardware is to plug, unplug, or switch a jumper on the motherboard (for "switching a jumper" I mean that you find a jumper that joins the central pin and a side pin of a group of three pins, you should then unplug the jumper and then plug it to the central pin and to the pin on the opposite side, so if the jumper is normally on position 1-2, you have to put it on position 2-3, or viceversa). This jumper is not always located near to the BIOS, but could be anywhere on the motherboard.
To find the correct jumper you should read the motherboard's manual.

Once you've located the correct jumper, switch it (or plug or unplug it, depending from what the manual says) while the computer is turned OFF. Wait a couple of seconds then put the jumper back to its original position. In some motherboards it may happen that the computer will automatically turn itself on, after flashing the BIOS. In this case, turn it off, and put the jumper back to its original position, then turn it on again. Other motherboards require you turn the computer on for a few seconds to flash the BIOS.
If you don't have the motherboard's manual, you'll have to "bruteforce" it... trying out all the jumpers. In this case, try first the isolated ones (not in a group), the ones near to the BIOS, and the ones you can switch (as I explained before). If all them fail, try all the others. However, you must modify the status of only one jumper per attempt, otherwise you could damage the motherboard (since you don't know what the jumper you modified is actually meant for). If the password request screen still appear, try another one.
If after flashing the BIOS, the computer won't boot when you turn it on, turn it off, and wait some seconds before to retry.

Removing the battery

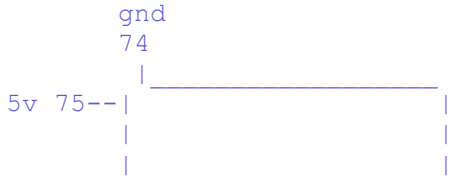
If you can't find the jumper to flash the BIOS or if such jumper doesn't exist, you can remove the battery that keeps the BIOS memory alive. It's a button-size battery somewhere on the motherboard (on elder computers the battery could be a small, typically blue, cylinder soldered to the motherboard, but usually has a jumper on its side to disconnect it, otherwise you'll have to unsolder it and then solder it back). Take it away for 15-30 minutes or more, then put it back and the data contained into the BIOS memory should be volatilized. I'd suggest you to remove it for about one hour to be sure, because if you put it back when the data aren't erased yet you'll have to wait more time, as you've never removed it. If at first it doesn't work, try to remove the battery overnight.
Important note: in laptop and notebooks you don't have to remove the computer's power batteries (which would be useless), but you should open your computer and remove the CMOS battery from the motherboard.

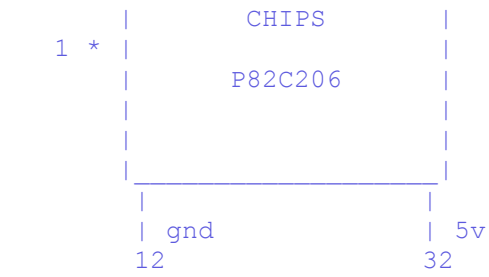
Short-circuiting the chip

Another way to clear the CMOS RAM is to reset it by short circuiting two pins of the BIOS chip for a few seconds. You can do that with a small piece of electric wire or with a bended paper clip. Always make sure that the computer is **turned OFF** before to try this operation.
Here is a list of EPROM chips that are commonly used in the BIOS industry. You may find similar chips with different names if they are compatible chips made by another brand. If you find the BIOS chip you are working on matches with one of the following you can try to short-cicuit the appropriate pins. **Be careful**, because this operation may damage the chip.

CHIPS P82C206 (square)

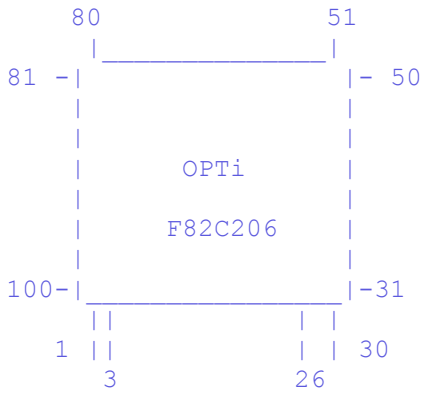
Short together pins 12 and 32 (the first and the last pins on the bottom edge of the chip) or pins 74 and 75 (the two pins on the upper left corner).





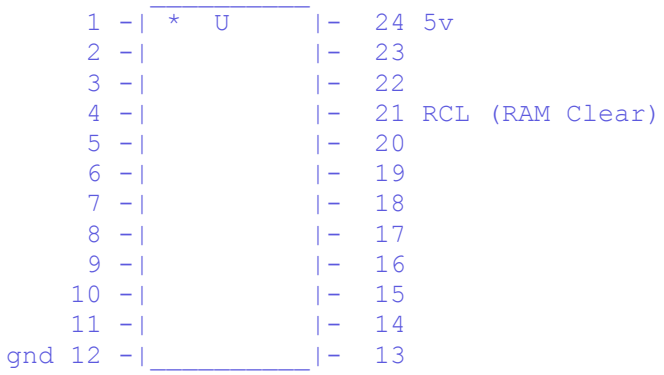
OPTi F82C206 (rectangular)

Short together pins 3 and 26 (third pin from left side and fifth pin from right side on the bottom edge).



Dallas DS1287, DS1287A
Benchmarq bp3287MT, bq3287AMT

The Dallas DS1287 and DS1287A, and the compatible Benchmarq bp3287MT and bq3287AMT chips have a built-in battery. This battery should last up to ten years. Any motherboard using these chips should not have an additional battery (this means you can't flash the BIOS by removing a battery). When the battery fails, the RTC chip would be replaced.
CMOS RAM can be cleared on the 1287A and 3287AMT chips by shorting pins 12 and 21.
The 1287 (and 3287MT) differ from the 1287A in that the CMOS RAM can't be cleared. If there is a problem such as a forgotten password, the chip must be replaced. (In this case it is recommended to replace the 1287 with a 1287A). Also the Dallas 12887 and 12887A are similar but contain twice as much CMOS RAM storage.

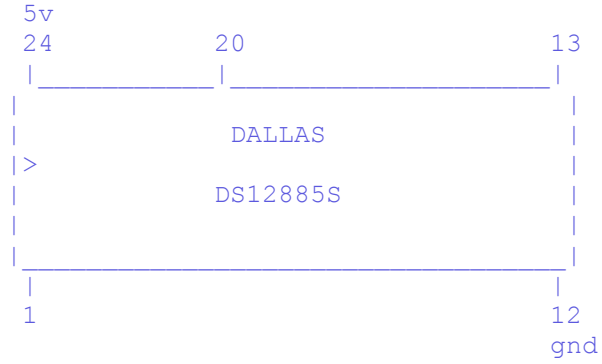


NOTE: Although these are 24-pin chips,

```
the Dallas chips may be missing 5 pins,
these are unused pins.
Most chips have unused pins,
though usually they are still present.
```

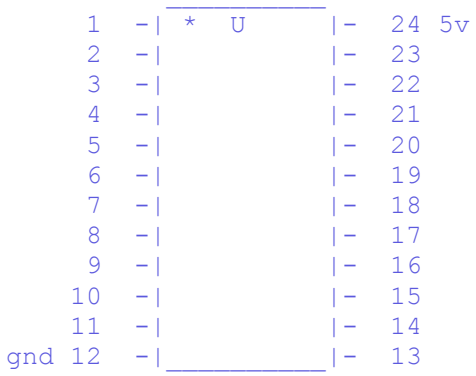
Dallas DS12885S
Benchmarq bq3258S
Hitachi HD146818AP
Samsung KS82C6818A

This is a rectangular 24-pin DIP chip, usually in a socket. The number on the chip should end in 6818.
Although this chip is pin-compatible with the Dallas 1287/1287A, there is no built-in battery.
Short together pins 12 and 24.



Motorola MC146818AP

Short pins 12 and 24. These are the pins on diagonally opposite corners - lower left and upper right. You might also try pins 12 and 20.



Replacing the chip

If nothing works, you could replace the existing BIOS chip with a new one you can buy from your specialized electronic shop or your computer supplier. It's a quick operation if the chip is inserted on a base and not soldered to the motherboard, otherwise you'll have to unsolder it and then put the new one. In this case would be more convenient to solder a base on which you'll then plug the new chip, in the eventuality that you'll have to change it again. If you can't find the BIOS chip specifically made for your motherboard,

you should buy one of the same type (probably one of the ones shown above) and look in your motherboard manufacturer's website to see if there's the BIOS image to download. Then you should copy that image on the chip you bought with an EPROM programmer.

Important

Whether is the method you use, when you flash the BIOS not only the password, but also all the other configuration data will be reset to the factory defaults, so when you are booting for the first time after a BIOS flash, you should enter the CMOS configuration menu (as explained before) and fix up some things.
Also, when you boot Windows, it may happen that it finds some new device, because of the new configuration of the BIOS, in this case you'll probably need the Windows installation CD because Windows may ask you for some external files. If Windows doesn't see the CD-ROM try to eject and re-insert the CD-ROM again. If Windows can't find the CD-ROM drive and you set it properly from the BIOS config, just reboot with the reset key, and in the next run Windows should find it. However most files needed by the system while installing new hardware could also be found in `C:\WINDOWS`, `C:\WINDOWS\SYSTEM`, or `C:\WINDOWS\INF` .

Key Disk for Toshiba laptops

Some Toshiba notebooks allow to bypass BIOS by inserting a "key-disk" in the floppy disk drive while booting. To create a Toshiba Keydisk, take a 720Kb or 1.44Mb floppy disk, format it (if it's not formatted yet), then use a hex editor such as Hex Workshop to change the first five bytes of the second sector (the one after the boot sector) and set them to 4B 45 59 00 00 (note that the first three bytes are the ASCII for "KEY" :) followed by two zeroes). Once you have created the key disk put it into the notebook's drive and turn it on, then push the reset button and when asked for password, press Enter. You will be asked to Set Password again. Press Y and Enter. You'll enter the BIOS configuration where you can set a new password.

Key protected cases

A final note about those old computers (up to 486 and early Pentiums) protected with a key that prevented the use of the mouse and the keyboard or the power button. All you have to do with them is to follow the wires connected to the key hole, locate the jumper to which they are connected and unplug it. That's all.