Microsoft CD Key Authentication Revealed!

(You won't see this on their MSDN Level 2 CD!)

You are Visitor Number 13275 since Feb. 8th, 1996

If you are interested in other information similar to the Microsoft CD Key, please check out the rest of
Damaged Cybernetics!

Abstract

This document will cover details about what makes up a Microsoft CD Keys and how they are authenticated. With the rush in of Windows'95, Microsoft has implemented a CD Key to either help foil piracy or to **track** their software thoughout the world. It was brought to my attention by a Microsoft Production Manager that they use this for their regional tracking, and also for product codes. They also understand the weakness of the key.

I find this a little bothersome. Here are some points...

- If you do not supply a valid CD key for the retail version of a Microsoft Product CD, you **cannot** install it. On the Upgrade version of the CD, you can click **Ignore**, but you need an older version of Windows installed.
- If this key is based on regional tracking, then how come there are people on the other side of the United States that have the same first 3 digits as several of my CDs? Is Microsoft so power hungry now that they are tracking by continent now?
- If this key is used for product codes, then how come my Plus Pack and Visual Basic Professional have the same first 3 digits? How does this seperate the two products?

If you can contribute any information about the Microsoft CD Key please inform us!.

Also we do acknowledge there is a small problem concerning with the authentication of the OEM keys. In some of our more extensive tests we discovered that the first 5 digits of the OEM key are actualy being used now.

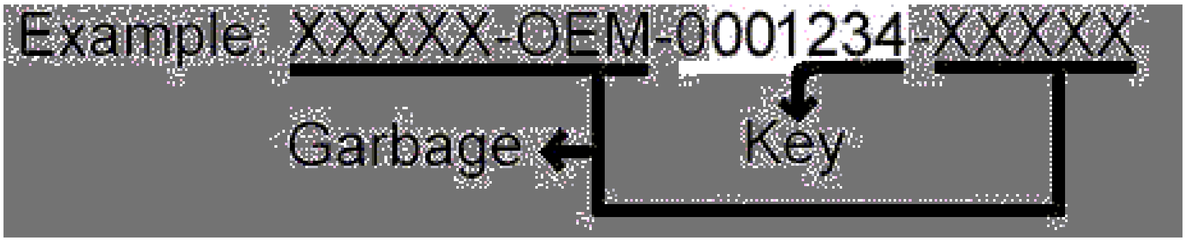
In either case, the CD Key is really a **hassle** on my part. I either lose the cases or my kids eat the sticker. *(Also those glossy cardboard sleeves are even worse.)* Great, how am **I** supposed to reinstall my software when my system crashes? Also if this **IS** being used as a scheme to foil **piracy**. It doesn't work, because one can **easily copy** the CD-Key as easy as the CD.

C Source code is provided to show how a key can be authenticated.

CD Key Details

- **CD Keys are interchangable between Microsoft Products employing this scheme. This means you can take your Windows'95 CD Key and reuse it on your Microsoft Office Professional CD or any other Microsoft CD!. This scheme also works with Developer Level 2 and Level 3 CDs.**
- **CD Keys contain alphanumeric characters, however the REAL key only contains numbers (0..9).**
- **There are 2 types of keys being used at the moment. One is for the retail version of the product, the other is for OEM bundled software.**
  The retail version of the key is split into two sets of characters. The first set is not needed in the authentication process. The second set contains nothing but digits. This is the set we need to authenticate. It is unknown what the first set characters are used for.
  Here is an example of a retail version of the key.
  

  The OEM version of the key is similar to the retail version, but with more alphanumeric characters This key is broken up into 4 sets of alphanumeric characters. The first, second and fourth sets are not used in the authentication process. The second set of characters contains the string 'OEM'. The third set of characters are all digits and is the set that used to authenticate the key. The first 3 digits of the third set must be ZERO, the last 4 digits can vary. It is unknown what the first and fourth set of characters are used for.
  Here is an example of an OEM version of the key.



- **In both types of keys, the order is not relative! (the part of the key that needs to be authenticated that is). Meaning that you can rearrange the order of the digits any way you like too and it would still produce a valid Microsoft CD Key! This is because the authentication is based on the SUM of the digits.**

Key Authentication

The algorithm to the authentication routine is a VERY simple one. One can write a small amount of source code that will randomly generate valid CD Keys. Lets use the following keys and follow the steps to authenticate them.

Our Microsoft Retail CD Key: 666-0077700
Our Microsoft OEM CD Key: 66666-OEM-0007770-66666

- Strip off the first set of characters in the retail version. In the OEM version strip off the first, second and fourth character sets. We are left with the following:
  Retail CD Key: 0077700
  OEM CD Key: 0007770 *(Note: first 3 digits MUST be ZERO!)*
- From here on out both keys can follow the same authentication algorithm. We do this by adding each digit one after another until we produce a sum.
  Retail CD Key: 0 + 0 + 7 + 7 + 7 + 0 + 0 = 21
  OEM CD Key: 0 + 0 + 0 + 7 + 7 + 7 + 0 = 21
- Now take the result modulus by 7. If result of the modulus operation is 0 then the key is consider to be a authentic Microsoft CD Key. Note that the algorithm is **MODULUS**, not **DIVISION**! Why? A key of 0000000 is considered to be authentic! If we follow the steps in authenticating this key, we would get a value of zero. A division by 0 will generate an exception as where a modulus will not.
  21 **MOD** 7 = 0

>