

Forum:[Hack Forums](#)

Thread: [\[VB.NET\] Make your own Keygen \[VB.NET\]](#)

void - January 29, 2010, 4:37 am

MAKE YOUR OWN KEYGEN

Tutorial by: *_void_*

Hello everyone today i will teach you how to make your own keygen.

Before we start i will like to tell you that there are alots of others advanced keygens but this one is basic. When you know how to create an advanced keygen that keygen will be real. So let's start.

Requirements:

1) [Visual Basic 2008](#)

2) New project ?

Ok let's start.

Step 1.

Open VB2008 click File>New Project

Step 2.

Add following:

1 Textbox

1 Button

Step 2.

Rename the button to "Generate"

Leave blank field at textbox

Spoiler ([Click to View](#))

Step 3.

Double click at "Generate"(Button1), and add this code:

Code `TextBox1.Text = Int(Rnd() * 4)`

 Select Case TextBox1.Text

 Case 0

 TextBox1.Text = "CD key"

 Case 1

 TextBox1.Text = "CD key"

 Case 2

 TextBox1.Text = "CD key"

 Case 3

 TextBox1.Text = "CD key"

 End Select
TIP: Remove the "CD key" (Don't remove quotes), and write anything you want. You can add even more.

E.G: Case 4

 TextBox1.Text = "H4G87-V87TB-487GB-G8748-G7473"

Spoiler ([Click to View](#))

Congratulations ! You did it !

Step 4.

Now click at File>Save All, and save it. Now click at Build>Build(your project name).

Now start debugging to see if it works.

Here is the source:

(Don't download if you don't trust me)

Code <http://h1.Spam.com/blabla21/Keygen.rar>

Code AgcPqKQmz0zdf7GGPassword encrypted with:Bse64,Gila7

Just a little Anti Noob/Leech protection.

Scan Report:

File Info

Report generated: 29.1.2010 at 13.34.24 (GMT 1)

Filename: Keygen.rar

File size: 779412 bytes

MD5 hash: ec4830e594d1859bbcf54c81d173b366

SHA1 hash: 27B65885AE737CB96FA47ACF18CD8ACABC86E18B

Detection rate: 1 on 24

Status: INFECTED

Detections

a-squared - -

Avira AntiVir - -

Avast - -

AVG - -

BitDefender - -

ClamAV - -

Comodo - -

Dr.Web - -

Ewido - -

F-PROT6 - -

G-Data - -

Ikarus T3 - -

Kaspersky - -

McAfee - -

NOD32 v3 - -

Norman - -

Panda - -

QuickHeal - -

Solo Antivirus - -

Sophos - Sus/Keygen-A

TrendMicro - -

VBA32 - -

VirusBuster - -

ZonerAntivirus - -

Scan report generated by

NoVirusThanks.org

Haha,it detects like keygen is in it ?.It will detect yours also once you build it.

Thank you for reading my tutorial.Any bugs/reports just comment.Leave feedback if you want

--([S7N-])-- - January 29, 2010, 4:43 am

Is this a fake keygen? Or does this actually activate the software you are trying to generate the keys of?

Sikandar - January 29, 2010, 4:43 am

remove that "+Rep if you want.Someone gave me -3"

void - January 29, 2010, 4:45 am

(Jan 29, 2010 05:43 AM)No0b Wrote: [\[CITE\]](#) Is this a fake keygen? Or does this actually activate the software you are trying to generate the keys of?Don't know.Try it.

(Jan 29, 2010 05:43 AM)sikandarnandwani Wrote: [\[CITE\]](#) remove that "+Rep if you want.Someone gave me -3"Removed.

Odayleet - January 29, 2010, 5:19 am

Thanks you :)

void - January 29, 2010, 5:22 am

(Jan 29, 2010 06:19 AM)Julie Wrote: [\[CITE\]](#) Thanks you :)Your welcome.Any bugs or troubles just tell.

Dead #45 - January 29, 2010, 5:22 am

Where i can get VB.NET, i have vb 6.0.Pm me with link please?

void - January 29, 2010, 5:32 am

(Jan 29, 2010 06:22 AM)NoRi Wrote: [\[CITE\]](#) Where i can get VB.NET, i have vb 6.0.Pm me with link please?

The download is where it says:

"1)Visual Basic 2008",click on the Visual Basic 2008 and you are going to download.The site is form Microsoft.

Xdem0 - January 29, 2010, 5:56 am

Not exactly a "KeyGen", as quoted, a keygen will generate keys. Not randomly display a preset key. The whole point of a keygen is to generate a serial from an algorithm (which is usually extracted from a piece of software).

This is more of a "Serial Listing application". No disrespect though, many keygens come in this format and can still prove useful. Good tutorial also. ;p

--([S7N])-- - January 29, 2010, 6:07 am

(Jan 29, 2010 06:56 AM)Xdem0 Wrote: [\[CITE\]](#) Not exactly a "KeyGen", as quoted, a keygen will generate keys. Not randomly display a preset key. The whole point of a keygen is to generate a serial from an algorithm (which is usually extracted from a piece of software).

This is more of a "Serial Listing application". No disrespect though, many keygens come in this format and can still prove useful. Good tutorial also. ;p

Exactly! That is why I thought it was a fake Keygen. This can make fake keygens more believable though.

void - January 29, 2010, 6:13 am

(Jan 29, 2010 06:56 AM)Xdem0 Wrote: [\[CITE\]](#) Not exactly a "KeyGen", as quoted, a keygen will generate keys. Not randomly display a preset key. The whole point of a keygen is to generate a serial from an algorithm (which is usually extracted from a piece of software).

This is more of a "Serial Listing application". No disrespect though, many keygens come in this format and can still prove useful. Good tutorial also. ;pYour welcome.Anyway it's good if you make a fake keygen for RAT's,Keyloggers,Bots and other stuffs.

(Jan 29, 2010 07:07 AM)No0b Wrote: [\[CITE\]](#) Exactly! That is why I thought it was a fake Keygen.

This can make fake keygens more believable though. You can find real serial and then enter into your fake keygen, and then record and send on youtube and put a download, so they can download your servers, and spread more easily.

void - January 29, 2010, 8:40 am

Any other comments ?

Ex-Coder - January 29, 2010, 9:04 am

Thanks dude :) I will start making fake keygens. HAHA

void - January 29, 2010, 9:16 am

(Jan 29, 2010 10:04 AM)h3lLx0x Wrote: [\[CITE\]](#) Thanks dude :) I will start making fake keygens. HAHA

Glad you like it. Start and spread your servers faster.

fleischi93 - January 29, 2010, 9:19 am

No one knows how to generate random numbers with capital letters?

I don't want to use the "Case method" I want to generate random numbers with capital letters on every click.

Like

0DK4-5KSE4-KE32-KU6RZ

But NOT the case method. I'd love to know how to do that..

Ex-Coder - January 29, 2010, 9:27 am

Do you mean generating random numbers that are not real ? randomly numbers?

You can make your own random key

Quote:TIP:Remove the "CD key"(Don't remove quotes),and write anything you want. You can add even more.

E.G:Case 4

TextBox1.Text = "H4G87-V87TB-487GB-G8748-G7473"

rowey-2k9 - January 29, 2010, 9:36 am

i have a code liein around somewhere fleischi93, ill PM you if i can find it

fleischi93 - January 29, 2010, 10:03 am

@h3lLx0x

Exactly. False random numbers. No algorithm or something. Just false random codes with numbers and capital letters

@rowey-2k9

That would be very nice :)

Cosmo??? - January 29, 2010, 10:11 pm

Dude, this ISN'T a KEYGEN. This does not GENERATE keys. This just says the keys you put,

otherwise it would use special algorithms to generate working keys.

CopyBoT - January 30, 2010, 12:21 am

(Jan 29, 2010 07:07 AM)No0b Wrote: [\[CITE\]](#) Exactly! That is why I thought it was a fake Keygen. This can make fake keygens more believable though.

Not a fake but randomly display a preset key .

Cracking an Algorithm and Coding a Keygen

Hello everyone, I have finally decided to write a new paper, I will publish it in my blog and provide it as .pdf too

So basically we're going to use a very easy keygenme, get the algorithm and then code a Keygen in Delphi and Assembler. You can use other languages, aslong as you can integrate Assembler in it.

The Target

The Target is Progressive Keygenme #1 which you can find at <http://membres.lycos.fr/stockage01/> it was created by fargoth.

Lets get started : Finding the Algorithm

I assume that you already know how to find the algorithm, if not, I recommend you to read & watch some tutorials about it, basically you need to step over the code with a Debugger until you find a loop-like place or anything unusual.

```
00401065 |. FF15 BE304000 CALL DWORD PTR DS:[
0040106B |. 83F8 05      CMP EAX,5
0040106E |. 72 7E      JB SHORT 004010EE
00401070 |. 83F8 14      CMP EAX,14
00401073 |. 0F87 8C000000 JA 00401105
00401079 |. 89C1      MOV ECX,EAX
0040107B |. 8D35 00204000 LEA ESI,DWORD PTR DS:[402000]
00401081 |. 31DB      XOR EBX,EBX
00401083 |> 0FB606      /MOVZX EAX,BYTE PTR DS:[ESI]
00401086 |. 01C3      |ADD EBX,EAX
00401088 |. 46      |INC ESI
00401089 |.^ E2 F8      \LOOPD SHORT 00401083
0040108B |. 53      PUSH EBX
```

Do you see this loop?(line 9 to 12) This is the algorithm that generates a key to check if the one you inputed matches the real one.

Now you can try to understand what it does, you could set some break points inside the loop and look at the registers to see what it actually does, that is a quick way if the algorithm is short.

However you should try to understand what the codes does, which requires a good knowledge of Assembler.

What does the code actually do?

Line 2: The Program compares the length of our name with 5(hex) which is 5 in decimal , and jumps if it is shorter.

Line 4: The Program compares the length of our name with 14(hex) which is 20 in decimal and jumps if it is longer than 14.

Line 8: EAX gets XOR'ed with EAX, which empties the Register

Line 9: The first byte from ESI (Where our String is located) is moved into EAX.

Line 10: The Ascii value of the character in EAX is added into EBX.

Line 12: We loop again

Line 13: EBX is pushed into the stack, this is our good serial.

Now we need to make a keygen for this Keygenme, I choosed to use Delphi / Pascal because it is very easy to program on it and it's the language I prefer.

Editing this rough code from Olly into Delphi

You cannot use the Virtualaddresses in Delphi because there is no offset and such things. Which means we need to hardcore the addresses. This took me a while to figure out because I had no tutorial.

I will create a console program because I do not need to create Textboxes which could confuse you oldschool ftw

For example the loop cannot be "LOOPD SHORT 00401083" because the address 00401083 doesn't exist anymore: so we need to define a function which will be called @keygen: and will contain the loop.

We also need to put pushad and popad, because if we don't, Delphi will kill itself and scream about violation error

This is the Delphi code which runs in Delphi 7 and on Delphi 2007.

Code program keygensolution;

var USERNAME:String;

LEN,SERIAL:Integer;

begin

write('Input your Username : ');

read(USERNAME);

LEN:=length(USERNAME);

ASM

PUSHAD

MOV ECX,EAX

XOR EAX,EAX

XOR EBX,EBX

MOV ESI,USERNAME

MOV ECX,LEN

@keygen:

MOVZX EAX,BYTE PTR DS:[ESI]

ADD EBX,EAX

INC ESI

LOOP @keygen

MOV SERIAL,EBX

POPAD

end;

writeln('The Serial is : ',SERIAL);

readln();

end.As you see this program isn't very complicated. It was copy-pasting and then adapting the addresses.

You could also have translated to assembler code into Pascal syntax, but when you make keygens for bigger algorithms, you loose quite some time

If you need help just reply to this post.

This entry was posted on February 5, 2008 at 12:44 pm and is filed under ASM, Delphi, Programming, Reverse Engineering with tags algorithm crack, assembler keygen, Cracking an Algorithm and Coding a Keygen, delphi assembler, keygen algorithm, keygen assembly, keygening. You can follow any responses to this entry through the RSS 2.0 feed You can leave a response, or trackback from your own site.

<http://usernamedenied.wordpress.com/2008/02/05/cracking-an-algorithm-and-coding-a-keygen/>

--([S7N])-- - January 30, 2010, 1:33 am

<http://usernamedenied.wordpress.com/2008/02/05/cracking-an-algorithm-and-coding-a-keygen/>

^That isn't VB.

void - January 30, 2010, 5:33 am

(Jan 30, 2010 02:33 AM)No0b Wrote: [\[CITE\]](#)

<http://usernamedenied.wordpress.com/2008/02/05/cracking-an-algorithm-and-coding-a-keygen/>

^That isn't VB. Yeah it isn't VB.

CopyBoT - January 30, 2010, 8:34 am

then code a Keygen in Delphi and Assembler. You can use other languages,

void - January 30, 2010, 12:09 pm

(Jan 30, 2010 09:34 AM)CopyBoT Wrote: [\[CITE\]](#) then code a Keygen in Delphi and Assembler. You can use other languages,

Well this isn't a real one, it's fake so you can use it for spreading.

Tate - January 30, 2010, 6:41 pm

(Jan 29, 2010 06:56 AM)Xdem0 Wrote: [\[CITE\]](#) Not exactly a "KeyGen", as quoted, a keygen will generate keys. Not randomly display a preset key. The whole point of a keygen is to generate a serial from an algorithm (which is usually extracted from a piece of software).

This is more of a "Serial Listing application". No disrespect though, many keygens come in this format and can still prove useful. Good tutorial also. ;p

Wow.

I know this is off topic to the post, but that was well helpful. I had no idea that's how keys were made. I thought it was just random, and then it added to a list, so if it was on the list, it couldn't be made again.

This might help me if I ever make a keygen.

void - January 30, 2010, 6:43 pm

(Jan 30, 2010 07:41 PM)Tate Wrote: [\[CITE\]](#) Wow.

I know this is off topic to the post, but that was well helpful. I had no idea that's how keys were made. I thought it was just random, and then it added to a list, so if it was on the list, it couldn't be made again.

This might help me if I ever make a keygen. Yeah, but you must have a highly in coding in visual basic. Once you done that make sure you use right algorithms. Good luck !

pushl %ebp - January 30, 2010, 6:50 pm

Nice tutorial, I like that you added colors. Petty that I don't associate myself near Visual Basics. ?

void - January 30, 2010, 7:03 pm

(Jan 30, 2010 07:50 PM)h4ckingURLife Wrote: [\[CITE\]](#) Nice tutorial, I like that you added colors. Petty that I don't associate myself near Visual Basics. ? Thanks, why don't you just start learning VB it will be good ?

