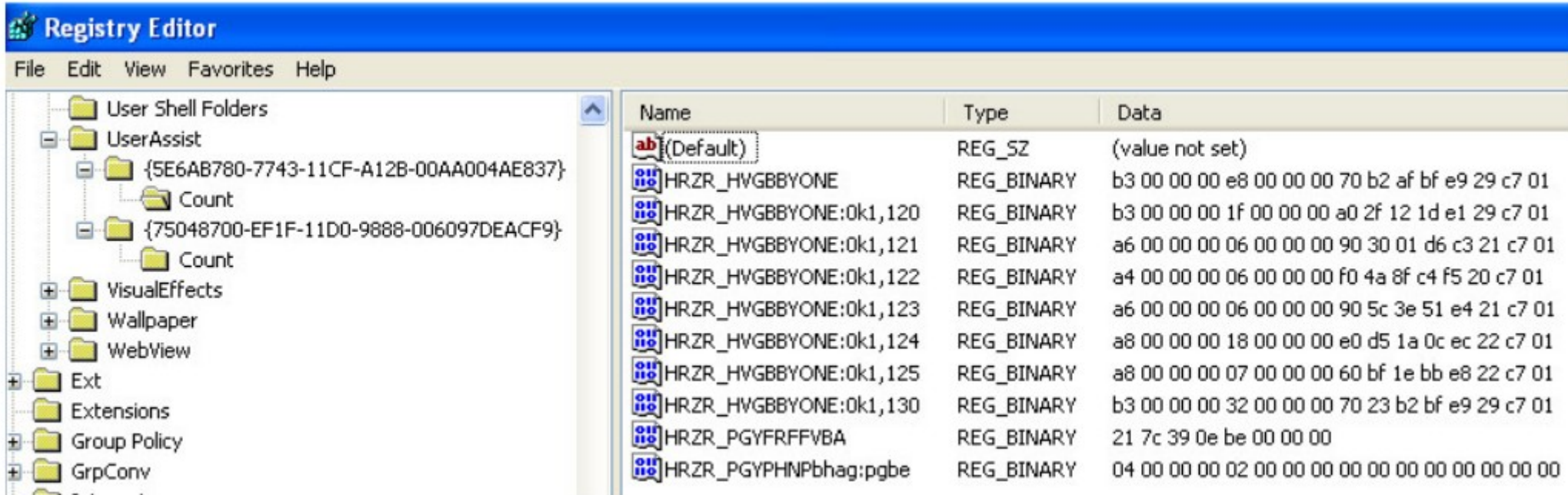


Windows 7: ROT13 or Vigenère? ;-)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count.



Registry Editor

File Edit View Favorites Help

User Shell Folders

- UserAssist
 - {5E6AB780-7743-11CF-A12B-00AA004AE837}
 - Count
 - {75048700-EF1F-11D0-9888-006097DEACF9}
 - Count
 - VisualEffects
 - Wallpaper
 - WebView
- Ext
- Extensions
- Group Policy
- GrpConv

Name	Type	Data
(Default)	REG_SZ	(value not set)
HRZR_HVGBBYONE	REG_BINARY	b3 00 00 00 e8 00 00 00 70 b2 af bf e9 29 c7 01
HRZR_HVGBBYONE:0k1,120	REG_BINARY	b3 00 00 00 1f 00 00 00 a0 2f 12 1d e1 29 c7 01
HRZR_HVGBBYONE:0k1,121	REG_BINARY	a6 00 00 00 06 00 00 00 90 30 01 d6 c3 21 c7 01
HRZR_HVGBBYONE:0k1,122	REG_BINARY	a4 00 00 00 06 00 00 00 f0 4a 8f c4 f5 20 c7 01
HRZR_HVGBBYONE:0k1,123	REG_BINARY	a6 00 00 00 06 00 00 00 90 5c 3e 51 e4 21 c7 01
HRZR_HVGBBYONE:0k1,124	REG_BINARY	a8 00 00 00 18 00 00 00 e0 d5 1a 0c ec 22 c7 01
HRZR_HVGBBYONE:0k1,125	REG_BINARY	a8 00 00 00 07 00 00 00 60 bf 1e bb e8 22 c7 01
HRZR_HVGBBYONE:0k1,130	REG_BINARY	b3 00 00 00 32 00 00 00 70 23 b2 bf e9 29 c7 01
HRZR_PGYFRFFVBA	REG_BINARY	21 7c 39 0e be 00 00 00
HRZR_PGYPHNPbhag:pgbe	REG_BINARY	04 00 00 00 02 00 00 00 00 00 00 00 00 00 00


Didier


 **Internet**
Mozilla Firefox

 **Launch Internet Explorer Browser**

 7-Zip File Manager

 Polar Precision Performance

 Microsoft Visual C# 2005 Express Edition

 Notepad

All Programs 

 **My Documents**

 **My Recent Documents** ▶


 **My Pictures**


 **My Music**

 **My Computer**


 **My Network Places**

 Control Panel

 Set Program Access and Defaults



 Connect To ▶

 Printers and Faxes

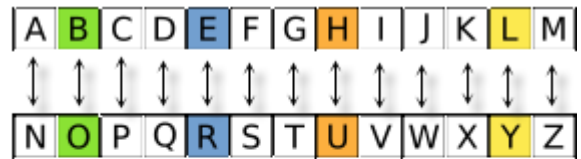
 Help and Support

 Search

 Run...

 Log Off  Shut Down

ROT13



UserAssist 2.1.0.0



Commands Help

Key	Index	Name	Unkno...	Session	Counter	Last
{5E6AB7...}	0	UEME_CTLSESSION	238398...	5		
{5E6AB7...}	1	UEME_CTLCUACount:ctor		1	2	
{750487...}	0	UEME_CTLSESSION	238239...	4		
{750487...}	7	UEME_CTLCUACount:ctor		1	2	
{750487...}	1	UEME_RUNPIDL:C:\Documents and Settings...		1	14	1/24/2006 4:29:24 PM
{750487...}	2	UEME_RUNPIDL:%csidl2%\MSN Explorer.lnk		1	13	1/24/2006 4:29:24 PM
{750487...}	3	UEME_RUNPIDL:%csidl2%\Windows Media ...		1	12	1/24/2006 4:29:24 PM
{750487...}	4	UEME_RUNPIDL:%csidl2%\Windows Messen...		1	11	1/24/2006 4:29:24 PM
{750487...}	5	UEME_RUNPIDL:%csidl2%\Accessories\Tour...		1	10	1/24/2006 4:29:24 PM
{750487...}	6	UEME_RUNPIDL:%csidl2%\Accessories\Win...		1	9	1/24/2006 4:29:24 PM
{5E6AB7...}	4	UEME_UITOOLBAR:0x4,7031		2	1	4/21/2006 4:23:20 PM
{750487...}	9	UEME_RUNCPL		4	1	4/25/2006 10:29:01 AM
{750487...}	10	UEME_RUNCPL:desk.cpl		4	1	4/25/2006 10:29:01 AM
{750487...}	14	UEME_RUNPATH:C:\Program Files\Microsoft...		4	2	4/25/2006 1:05:10 PM
{750487...}	11	UEME_RUNPIDL		4	10	4/26/2006 2:24:32 PM
{750487...}	13	UEME_RUNPIDL:%csidl2%\Microsoft Visual C...		4	4	4/26/2006 2:24:32 PM
{750487...}	15	UEME_RUNPIDL:%csidl2%		4	2	4/26/2006 2:24:32 PM
{750487...}	16	UEME_RUNPATH:D:\setup.exe		4	1	4/26/2006 2:55:34 PM
{750487...}	18	UEME_RUNPATH:C:\WINDOWS\regedit.exe		4	1	8/2/2006 1:16:03 PM
{750487...}	12	UEME_RUNPATH:C:\WINDOWS\system32\...		4	2	8/2/2006 1:17:50 PM
{750487...}	17	UEME_RUNPATH:C:\Program Files\Common ...		4	5	8/2/2006 4:54:10 PM
{5E6AB7...}	2	UEME_UITOOLBAR		5	6	8/2/2006 5:00:14 PM
{5E6AB7...}	3	UEME_UITOOLBAR:0x1,130		5	5	8/2/2006 5:00:14 PM
{750487...}	8	UEME_RUNPATH		4	21	8/3/2006 2:50:54 PM
{750487...}	19	UEME_RUNPATH:C:\Documents and Setting...		4	1	8/3/2006 2:50:54 PM

Windows 7 – Windows 2008 R2 Beta

Key	Index	Name	Unknown	Session	Counter
{CEBFF5...	0	MICROSOFT.WINDOWS.GETTINGSTARTED			
{CEBFF5...	1	UEME_CTLSESSION			
{CEBFF5...	2	MICROSOFT.WINDOWS.MEDIACENTER			
{CEBFF5...	3	C:\WINDOWS\SYSTEM32\STIKYNOT.EXE			
{CEBFF5...	4	C:\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE			
{CEBFF5...	5	C:\WINDOWS\SYSTEM32\CALC.EXE			
{CEBFF5...	6	C:\WINDOWS\SYSTEM32\MSPAINT.EXE			
{CEBFF5...	7	C:\USERASSIST.EXE			
{CEBFF5...	8	C:\WINDOWS\EXPLORER.EXE			
{F4E57C...	0	%CSIDL23%\ACCESSORIES\WELCOME CENTER.LNK			
{F4E57C...	1	UEME_CTLSESSION			
{F4E57C...	2	%CSIDL23%\MEDIA CENTER.LNK			
{F4E57C...	3	%CSIDL23%\ACCESSORIES\STICKY N...			
{F4E57C...	4	%CSIDL23%\ACCESSORIES\SNIPPING...			
{F4E57C...	5	%CSIDL23%\ACCESSORIES\CALCULA...			
{F4E57C...	6	%CSIDL23%\ACCESSORIES\PAINT.LN...			

The Registry Editor window is open, showing the path `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\UserAssist`. The right pane shows the list of values under this key, including the 'Count' value which is highlighted.

Name
(Default)
D:\KfokErqnke.vdb
D:\Mvxxsvq\jpsvjft.ygs
D:\Mvxxsvq\kjekkj32\BbxxkkocAebv.iwc
D:\Mvxxsvq\kjekkj32\BhxstPpp.uko
D:\Mvxxsvq\kjekkj32\loak.gya
D:\Mvxxsvq\kjekkj32\vgeidpu.lnr
D:\Mvxxsvq\wibcuoeu.nlt
Nejhbchjs.Baypfcj.YchxvbUuwjrn
Nejhbchjs.Baypfcj.PymwpKzpuay
VATU_MMPRCXTAE

Vigenère?

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Programmers Joke?
- Easter Egg?

It's a testing plan!

- **Steve Riley:** *Changing the encoding from ROT-13 to Vigenère makes it easier for us to test that we're getting the behavior we want — it's obvious if old data carries over, because ROT-13ed data makes no sense to Vigenère. This is very useful in pre-release builds while we're shaking the bugs out. However, there's no such benefit to using Vigenère in the final release — it doesn't convey the same message as ROT-13, and since it's key-based, it's easy to mistake Vigenère for true encryption. Therefore, in the final release of Windows 7, we'll revert to using ROT-13 for UserAssist.*

Conclusion

- Windows 7 and 2008 R2 Beta use Vigenère
- Windows 7 and 2008 R2 RTM use ROT13

<http://blog.DidierStevens.com/?s=userassist>