

## Re: OT| U.S. democracy in peril

**Source:** <http://sci.tech-archive.net/Archive/sci.space.policy/2004-11/1458.html>

---

**From:** Rand Simberg (*simberg.interglobal\_at\_org.trash*)

**Date:** 11/12/04

Date: Fri, 12 Nov 2004 03:18:01 GMT

On Fri, 12 Nov 2004 01:12:47 +0100, in a place far, far away, Andrew Nowicki <andrew@nospam.com> made the phosphor on my monitor glow in such a way as to indicate that:

>"Dr. Avi Rubin is currently Professor of Computer Science at John  
>Hopkins University. He accidentally got his hands on a copy of the  
>Diebold software program -- Diebold's source code -- which runs  
>their e-voting machines.  
>  
>Dr. Rubin's students pored over 48,609 lines of code that make up  
>this software. One line in particular stood out over all the rest:  
>  
>#define DESKEY ((des\_key\*) "F2654hd4")  
>  
>All commercial programs have provisions to be encrypted so as to  
>protect them from having their contents read or changed by anyone not  
>having the key. The line that staggered the Hopkin's team was that the  
>method used to encrypt the Diebold machines was a method called  
>Digital Encryption Standard (DES), a code that was broken in 1997 and  
>is NO LONGER USED by anyone to secure programs. F2654hd4 was the key  
>to the encryption. Moreover, because the KEY was IN the source code,  
>all Diebold machines would respond to the same key.  
>  
>I can't believe there is a person alive who wouldn't understand the  
>reason this was allowed to happen. This wasn't a mistake but a fixed  
>election."

<rolling eyes at whacko conspiracy monger?

Yeah, tell it to the Marines...