

# Re: Analog Hole Bill Would Require Secret Tech No One Can Examine

---

*Source:* <http://sci.tech-archive.net/Archive/sci.electronics.design/2006-01/msg04653.html>

---

- *From:* Joseph2k <joseph2k@xxxxxxxxxx>
  - *Date:* Thu, 26 Jan 2006 04:46:41 GMT
- 

Joerg wrote:

> Hello John,  
>  
>  
>>>That would last a week or so. By then some kid would have found out how  
>>>to hack it anyway.  
>>  
>> That's an unfortunate assumption. I hear it a lot, and I'd like to hear  
>> it a lot less, because it isn't even valid.  
>>  
>  
> That's what Bill Gates' engineers always thought as well.  
>  
>  
>> Nobody has managed to crack VideoCipher encryption on C-band satellite  
>> TV, despite the fact that it's been around since, when, the 1980s?  
>>

You must have forgot about the "captain midnight" episode. The perpetrator even overrode the uplink. Boxes were available in the 1990's but have disappeared since.

>  
> Ahem. A friend of ours was inquiring about the cost of sat TV south of  
> the border. He was told that he'd just have to buy these things here and  
> from then it's free. Sometimes it may quit. Then he should just come  
> back and it'll be fixed for free, they said. That was a shop that's been  
> around a while, not from the back of a truck.  
>  
>  
>> Nobody managed to crack the triple-DES protection on Divx DVDs.  
>>

No silicon is available that will do triple-DES at video rates. Therefore triple-DES is used for key management. That key and the encryption algorithm MUST be cheap enough for inclusion in consumer equipment (no more than \$1 in volume). Please checkout Linux Xvid algorithms which are

Re: Analog Hole Bill Would Require Secret Tech No One Can Examine

purportedly compatible.

>> No private entity has managed to crack PCS or GSM encryption... or if  
>> they have, they've kept it damned quiet.

There is no encryption there to crack.

>>  
>> When they start to get serious about HDMI content protection, I wouldn't  
>> be surprised if nobody ever cracks that, either, except by using gray-  
>> market chipsets whose keys will probably be revoked at the first sign of  
>> popularity.  
>>

You misunderstand the always fatal flaw in mass marketed encryption. It must always be cheap enough to sell, therefore it will never be strong enough to actually protect.

>  
> In the end it's all a question of market size for bootleg stuff. If  
> large enough, someone may eventually hack.  
>  
>  
>> It is not a good idea to rely on the generosity of hackers to fight  
>> unfair and unconstitutional laws for you. Only stupidly-weak or broken  
>> encryption (e.g., CSS on DVDs or or WEP on WiFi) can be cracked by, or  
>> on behalf of, consumers. The industry is rapidly evolving resistance to  
>> that kind of stupidity. We won't see another CSS-quality implementation  
>> on HD-DVD or BluRay... you can bet on that. If they want to control how  
>> you use it, they will.  
>>

Actually we already have.

>  
> I don't use any bootleg stuff. For moral reasons and also because  
> today's entertainment is mostly rather disgusting in nature. We do not  
> even own a DVD player. But I resent it when stuff prevents me from  
> normal and legal use of equipment. Or when some gvt slaps an automatic  
> guilt assumption penalty on regular gear, like the copyright tax that  
> Germany wants to leverage on all new PCs. That's wrong. I hope the  
> voters there will be smart next time.  
>

Mostly agreed, it is one of the reasons i use Linux.

> Regards, Joerg  
>  
> <http://www.analogconsultants.com>  
reply interstitial

—

JosephKK

---

• **Follow-Ups:**

- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Keith Williams
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Frithiof Andreas Jensen
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Michael A. Terrell

• **References:**

- ◆ **Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Winfield Hill
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Larkin
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: cs\_posting
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Larkin
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Miles
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Larkin
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Miles
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Joerg
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: John Miles
- ◆ **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**  
◇ From: Joerg

- Prev by Date: **Re: Annual Power Consumption Summary**
- Next by Date: **Re: small signal NPN transistor for muting microphone**
- Previous by thread: **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**
- Next by thread: **Re: Analog Hole Bill Would Require Secret Tech No One Can Examine**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**