= AACS encryption key controversy =

A controversy surrounding the AACS cryptographic key arose in April 2007 when the Motion Picture Association of America and the Advanced Access Content System Licensing Administrator , LLC (AACS LA) began issuing cease and desist letters to websites publishing a 128 @-@ bit (16 @-@ byte) number , represented in hexadecimal as 09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0 (commonly referred to as 09 F9) , a cryptographic key for HD DVDs and Blu @-@ ray Discs . The letters demanded the immediate removal of the key and any links to it , citing the anti @-@ circumvention provisions of the United States Digital Millennium Copyright Act (DMCA) .

In response to widespread Internet postings of the key , the AACS LA issued various press statements , praising those websites that complied with their requests as acting in a " responsible manner " , warning that " legal and technical tools " were adapting to the situation .

The controversy was further escalated in early May 2007 , when aggregate news site Digg received a DMCA cease and desist notice and then removed numerous articles on the matter and banned users reposting the information . This sparked what some describe as a digital revolt or " cyber @-@ riot " , in which users posted and spread the key on Digg , and throughout the Internet en masse , thereby leading to a Streisand effect . The AACS LA described this situation as an " interesting new twist " .

= = Background = =

Hexadecimal is a base @-@ 16 numeral system used in the fields of computer programming and mathematics . The key is an ordinary number most widely known by its hexadecimal representation ; in decimal notation , it is 13 @,@ 256 @,@ 278 @,@ 887 @,@ 989 @,@ 457 @,@ 651 @,@ 018 @,@ 865 @,@ 901 @,@ 401 @,@ 704 @,@ 640 .

Because the encryption key may be used as part of circumvention technology forbidden by the DMCA , its possession and distribution has been viewed as illegal by the AACS , as well as by some legal professionals . Since it is a 128 @-@ bit numerical value , it was dubbed an illegal number . Opponents to the expansion of the scope of copyright criticize the idea of making a particular number illegal .

Commercial HD DVDs and Blu @-@ ray Discs integrate copy protection technology specified by the AACS LA . There are several interlocking encryption mechanisms , such that cracking one part of the system does not necessarily crack other parts . Therefore , the " 09 F9 " key is only one of many parts that are needed to play a disc on an unlicensed player .

The AACS system can be used to revoke a key of a specific playback device , after it is known to have been compromised , as it has for WinDVD . The compromised players can still be used to view old discs , but not newer releases without encryption keys for the compromised players . If other players are then cracked , further revocation would lead to legitimate users of compromised players being forced to upgrade or replace their player software or firmware in order to view new discs . Each playback device comes with a binary tree of secret device and processing keys . The processing key in this tree , a requirement to play the AACS encrypted discs , is selected based on the device key and the information on the disc to be played . As such , a processing key such as the " 09 F9 " key is not revoked , but newly produced discs cause the playback devices to select a different valid processing key to decrypt the discs .

= = Timeline of AACS cracking = =

= = = 2006 = = =

On December 26 , 2006 , a person using the alias muslix64 published a utility named BackupHDDVD and its source code on the DVD decryption forum at the website Doom9 . BackupHDDVD can be used to decrypt AACS protected content once one knows the encryption key. muslix64 claimed to have found title and volume keys in main memory while playing HD DVDs using a software player , and that finding them is not difficult .

= = = 2007 = = =

On January 1 , 2007 , muslix64 published a new version of the program , with volume key support . On January 12 , 2007 , other forum members detailed how to find other title and volume keys , stating they had also found the keys of several movies in RAM while running WinDVD .

On or about January 13 , a title key was posted on pastebin.com in the form of a riddle , which was solved by entering terms into the Google search engine . By converting these results to hexadecimal , a correct key could be formed . Later that day , the first cracked HD DVD , Serenity , was uploaded on a private torrent tracker . The AACS LA confirmed on January 26 that the title keys on certain HD DVDs had been published without authorization .

Doom9.org forum user arnezami found and published the " 09 F9 " AACS processing key on February 11 :

Nothing was hacked , cracked or even reverse engineered btw : I only had to watch the " show " in my own memory . No debugger was used , no binaries changed .

This key is not specific to any playback device or DVD title . Doom9.org forum user jx6bpm claimed on March 4 to have revealed CyberLink 's PowerDVD 's key , and that it was the key in use by AnyDVD .

The AACS LA announced on April 16 that it had revoked the decryption keys associated with certain software high @-@ definition DVD players , which will not be able to decrypt AACS encrypted disks mastered after April 23 , without an update of the software .

On May 17 , one week before any discs with the updated processing key had reached retail , claims were reported of the new keys having been retrieved from a preview disc of The Matrix Trilogy . On May 23 , the key 45 5F E1 04 22 CA 29 C4 93 3F 95 05 2B 79 2A B2 was posted on Edward Felten 's Freedom to Tinker Blog and confirmed a week later by arnezami on Doom9 as the new processing key (MKB v3) .

= = = 2008 = = =

In August , two new processing keys were posted :

F1 90 A1 E8 17 8D 80 64 34 94 39 4F 80 31 D9 C8 , for MKB v4 , and

7A 5F 8A 09 F8 33 F7 22 1B D4 1F A6 4C 9C 79 33 , which appeared to work with MKB v6 , MKB v7 and MKB v8 discs .

= = = 2009 = = =

In March , two additional processing keys were posted :

C8 72 94 CE 84 F9 CC EB 59 84 B5 47 EE C1 8D 66 , for MKB v9

45 2F 6E 40 3C DF 10 71 4E 41 DF AA 25 7D 31 3F , for MKB v10

While individual discs have been decrypted containing media key block version 17 , processing keys for versions past 10 have not yet been released to the public .

Many more later keys were discovered , but most were not released publicly , probably because that would make them easier to revoke .

= = DMCA notices and Digg = =

As early as April 17 , 2007 , AACS LA had issued DMCA violation notices , sent by Charles S. Sims of Proskauer Rose . Following this , dozens of notices were sent to various websites hosted in the United States .

On May 1 , 2007 , in response to a DMCA demand letter , technology news site Digg began closing accounts and removing posts containing or alluding to the key . The Digg community reacted by creating a flood of posts containing the key , many using creative ways of semi @-@ directly or indirectly inserting the number , such as in song or images (either representing the digits pictorially or directly representing bytes from the key as colors) or on merchandise . At one point , Digg 's " entire homepage was covered with links to the HD @-@ DVD code or anti @-@ Digg references . " Eventually the Digg administrators reversed their position , with founder Kevin Rose stating :

But now , after seeing hundreds of stories and reading thousands of comments , you 've made it clear . You 'd rather see Digg go down fighting than bow down to a bigger company . We hear you , and effective immediately we won 't delete stories or comments containing the code and will deal with whatever the consequences might be .

= = = Legal opinions = = =

Lawyers and other representatives of the entertainment industry , including Michael Ayers , an attorney for Toshiba Corporation , expressed surprise at Digg 's decision , but suggested that a suit aimed at Digg might merely spread the information more widely .

If you try to stick up for what you have a legal right to do , and you 're somewhat worse off because of it , that 's an interesting concept .

The American Bar Association 's eReport published a discussion of the controversy , in which Eric Goldman at Santa Clara University 's High Tech Law Institute noted that the illegality of putting the code up is questionable (that Section 230 of the Communications Decency Act may protect the provider when the material itself is not copyrighted) , although continuing to allow posting of the key may be " risky " , and entertainment lawyer Carole Handler noted that even if the material is illegal , laws such as the DMCA may prove ineffective in a practical sense .

= = Impact = =

In a response to the events occurring on Digg and the call to " Spread this number " , the key was rapidly posted to thousands of pages , blogs and wikis across the Internet . The reaction was an example of the Streisand effect .

Intellectual property lawyer Douglas J. Sorocco noted , " People are getting creative . It shows the futility of trying to stop this . Once the information is out there , cease @-@ and @-@ desist letters are going to infuriate this community more . " Outside the Internet and the mass media , the key has appeared in or on T @-@ shirts , poetry , songs and music videos , illustrations and other graphic artworks , tattoos and body art , and comic strips .

On Tuesday afternoon , May 1 , 2007 , a Google search for the key returned 9 @,@ 410 results , while the same search the next morning returned nearly 300 @,@ 000 results . On Friday , the BBC reported that a search on Google shows almost 700 @,@ 000 pages have published the key , despite the fact that on April 17 , the AACS LA sent a DMCA notice to Google , demanding that Google stop returning any results for searches for the key .

Widespread news coverage included speculation on the development of user @-@ driven websites , the legal liability of running a user @-@ driven website , the perception of acceptance of DRM , the failure as a business model of " secrecy based businesses ... in every aspect " in the Internet era , and the harm an industry can cause itself with harshly @-@ perceived legal action .

In an opposing move , Carter Wood of the National Association of Manufacturers said they had removed the " Digg It " -link from their weblog .

Until the Digg community shows as much fervor in attacking intellectual piracy as attacking the companies that are legitimately defending their property , well , we do not want to be promoting the site by using the " Digg It " feature .

Media coverage initially avoided quoting the key itself . However , several US @-@ based news sources have run stories containing the key , quoting its use on Digg , though none are known to have received DMCA notices as a result . Later reports have discussed this , quoting the key . Current TV broadcast the key during a Google Current story on the Digg incident on May 3 , 2007 , displaying it in full on screen for several seconds and placing the story on the station website .

Wikipedia , on May 1 , 2007 , locked out the page named for the number " to prevent the former secret from being posted again . The page on HD DVD was locked , too , to keep out The Number . " This action was later reversed .

= = = AACS LA reaction = = =

On May 7 , 2007 , the AACS LA announced on its website that it had " requested the removal solely of illegal circumvention tools , including encryption keys , from a number of web sites " , and that it had " not requested the removal or deletion of any ... discussion or commentary " . The statement continued , " AACS LA is encouraged by the cooperation it has received thus far from the numerous web sites that have chosen to address their legal obligations in a responsible manner . " BBC News had earlier quoted an AACS executive saying that bloggers " crossed the line " , that AACS was looking at " legal and technical tools " to confront those who published the key , and that the events involving Digg were an " interesting new twist " .