Journal of Information, Law and Technology

Trouble with Prime Numbers: DeCSS, DVD and the Protection of Proprietary Encryption Tools

Andrés Guadamuz González
Law Lecturer
University of Edinburgh

a.guadamuz@ed.ac.uk

This is a **refereed** article published on: 6 December 2002

Citation: Guadamuz A, 'Trouble with Prime Numbers: DeCSS, DVD and the Protection of Proprietary Encryption Tools', *The Journal of Information, Law and Technology (JILT)* 2002 (3) <http://elj.warwick.ac.uk/jilt/02-3/guadamuz.html>

Abstract

The DVD video format has become one of the most important developments in the home entertainment market since the popularisation of the magnetic video recording. The film industry delivered this format with a built in security system which was supposed to avoid illegal copying of the discs, much as what is taking place with the music CD and the almost indiscriminate copying of music into MP3 format over the Internet. This was achieved by means of encryption technology.

This essay deals with the cracking of DVD encryption and its further diffusion as a computer programme named DeCSS, which has been made available over the Internet in various formats, including t-shirts and a numerical representation of the code. There are three court cases based on the online posting of this programme, two in the United States and one in Norway. The article starts by describing the technology involved, as it is felt by the author that some of these technical issues are of importance to the legal implications of the case and should be understood properly. The article then deals with the developments in all of the three cases up to this date. The essay then finishes with a look at the legal issues involved, including hyper-linking, trade secrets, freedom of speech and the translation of DeCSS into numerical format.

Keywords:

1. Introduction

In 1999, an interesting case started to develop in the uncharted fringes of the World Wide Web. A computer programmer from Norway managed to crack the encryption technology used to protect the innovative and increasingly popular Digital Versatile Disk (DVD) video technology. Soon after, the instructions to override the inbuilt protection of DVD discs were being distributed through countless web sites around the world. The legal battle is probably one of the most underreported decisions on the growing caseload that is shaping the picture of copyright protection on a digital environment, but this case is important because it has the potential to define many interesting subjects in different areas of the Internet, such as hyper-linking, freedom of speech and copyright.

The case would seem to be very straightforward at first glance; the movie industry claims that the hackers have wilfully misappropriated trade secrets by means of reverse engineering, and have applied for injunction orders against the sites that provide explanations on how to circumvent the existing technology.

However, this case is not a normal copyright infringement one, what makes it important for the legal profession is the nature of the encryption technology at the heart of the debate. This case also deals with the ingenuity of programmers in finding new ways of making public information which some courts have been found to infringe copyright. An example of this can be found in a series of long prime numbers. These are prime numbers that can be decoded to represent DeCSS; the program that can decrypt the information contained in any DVD disc, and therefore copy it. This poses some interesting questions.

Could the courts forbid sites from posting these numbers? What about the many other forms of representation of DeCSS code?

This case has been overshadowed by other high profile intellectual property cases in cyberspace, such as the Napster copyright saga, software patents and cyber squatting, and the reporting of this in this case has been surprisingly scarce in legal journals. Nevertheless, its importance cannot be underestimated because the definitions that may come from this case may be felt in other areas of intellectual property.
The present paper examines some of the legal issues involved in this case, but some of the technical aspects surrounding the cracking of DVD protection deserve a considerable amount of coverage as well, as it is it is felt by the author that these there is a misunderstanding of the technical aspects of the protection involved.

2. DVD and Encryption Technology

2.1 DVD Explained

The Digital Versatile Disk (DVD) video format is undoubtedly the most important development in video technology since the adoption of VHS format as the standard for manufacture and retail of home entertainment. The industry is abuzz with the possibilities that the new format provides, and the sale of home videos has been boosted by the introduction of discs that provide the highest digital quality and richness of content.

In general, the DVD format is an optical reading medium that allows for massive storage capacity in a two-sided disc the size of normal audio or computer Compact Disc (CD). The highest possible storage of a DVD is seventeen gigabytes, as compared to 600-700 megabytes of the traditional CD format.

The DVD format makes use of multimedia compression technology, which allows a user to store large amounts of information in a smaller space than it would normally take, making it possible to develop smaller and more efficient media storage and playback mediums. In general, higher compression rates translate into lower quality, and vice versa. The Moving Picture Experts Group (MPEG) developed in 1990 two different levels of compression, the MPEG level 1 for video and level 2 for digital television; DVD uses the second level, called MPEG-2.
MPEG-2 is also used in other types of information-rich digital content, such as digital cable television, high-definition television (HDTV) and small dish television (DSS). The difference between these formats and DVD is that it allows for a variable bit-rate compression scheme, which allows the person making the decision of how much space to use to change from high resolution/low compression to the opposite as required by the different types of video. These variations of detail allow the producers of a DVD disc to use higher compressions for less important scenes, and lower ones for high-detail action scenes, allowing for larger amounts of content on the DVD. At the same time as the compression of video, the format allows to store various sorts of audio tracks with the highest quality.

This versatility is what is making the DVD format so attractive for use on the home entertainment market. Most commercial DVDs come with various extra features that make them very appealing for the average consumer. Such features include various audio formats, the possibility of using multiple languages in the audio, inclusion of full movie commentary by the actors, director or producers, behind the scenes footage, movie trailers and multimedia-heavy presentations on the filmography of those involved in the production. Other advantages of the format include durability of the discs in comparison to videotapes.

DVD can be incorporated to a personal computer, with the advantage that it is set to replace the normal CD-ROM drives in the near future, most new computers now ship with a DVD-ROM instead of the old CD-ROM set. This allows computer users can watch movies in their systems, as well as use DVD-ROM multimedia CDs, which allow for larger content. Another feature is backward compatibility, as DVD-ROMs can read old CD-ROMs.

There is no doubt that DVD is experiencing increasing popularity, and is gaining a larger share of the market. In 1997, DVD player sales in the United States amounted to 700 thousand (including players and DVD-ROM). In 2000, the amount of players sold was of 8.5 million, and worldwide the amount of DVD-ROM drives was of 46 million. In 1998, there were only 2,200 DVD titles available; in 2000, the amount of titles was of over 10,000. In the UK alone, it is calculated that the sales of DVD titles in December 2000 exceeded all those of the previous year. In January of last year, DVD sales topped VHS sales for the first time in the United States, and the figures are likely to continue going up.

2.2 Encryption

One of the features that made DVD so appealing to the movie industry was its security when compared to other video formats, such as videotapes, which are easy to copy. DVD has an inbuilt security system called the Content Scrambling System (CSS), which uses encryption as a means of making sure people cannot copy the contents of the disc.

What exactly is encryption? In short, encryption is:

> '*the use of secret codes and ciphers to scramble information so that it is worthless to anybody but the intended recipients'.*

In computing, encryption makes use of mathematical formulae or algorithms to scramble the original data, this information can only be unscrambled by the use of a key, which is the set of mathematical instructions used to encrypt the information. Digital information, such as the one stored in a DVD disc, can be easily encrypted because the data is stored in numerical format by means of binary code (1s and 0s), so the key simply scrambles the existing numbers by applying the formula. A person who does not have the right key to unlock the data will only obtain a set of useless numbers.

Generally, two major types of encryption exist, by private key (also known as asymmetric or asynchronous) or by public key (also known as symmetric or synchronous). The

simplest way is using asymmetric key encryption, where a formula is used to scramble the information in the origin, and the same key is used to unscramble it. In public key encryption, both parts are given a pair of keys, a public one and a private one. The person scrambling the information looks up the recipient's key from a public directory, and then scrambles it using that key, but only the intended recipient can look at the data by decrypting it using his private key. The larger the keys, the better the encryption, this is because a person would have to go through a larger set of mathematical operations to try to guess what the key is. Keys are composed of bits of information, which describe the operation that is being performed on the original data. The amount of possibilities is exponential, an 8-bit key has 256 possible values, but a 20-bit key has 1,048,576 possible values. Most commercial encryption (such as the one found in web-browsers) uses 128-bit encryption.

The CSS method used by DVD manufacturers uses an even stronger variation of public key encryption to scramble the original video data, known as authentication. This means that to have access to the keys themselves you need to be authorised to do so by means of another key, called the authentication key. This is a 40-bit key that is unique to each DVD player manufacturer, be it software or hardware. Every single DVD disc contains a set of at least 400 such keys, and each player has a built-in one. The player uses its key to unlock the information inside the disc and allow playback.
By encrypting the information inside a DVD, manufacturers had a way to ensure that users could not copy their product. The encrypted information could in fact be copied onto a recordable CD or a computer, but the new CD would lack the keys to be unlocked (because the keys themselves are encrypted), so the user would not be able to see any information from the recorded source, rendering the copy useless.

2.3 Cracking DVD Protection

By 1999, the movie industry seemed content enough with CSS technology applied to DVD to continue to encourage the growth of the new video format, but other applications for the format were not being exploited yet, such as DVD music or DVD-ROM software.

However, the faith of the industry in the security of CSS was misplaced. In hindsight, it seems naïve that a 40-bit encryption, although relatively secure, would stop determined hackers and crackers from trying to attack it, as it can be easily circumvented.

However, the breaking of DVD encryption did not result from an attack by crackers; it came to be inspired by more innocent reasons. For various commercial motives, and due to the unique nature of the software, the Linux operating system did not have a DVD player, which meant that thousands of users of this system had to migrate to another operating system if they wanted to watch their DVDs with their computers. For anybody who is familiar with the cultist nature of Linux users and their almost mythical despise for Microsoft's products, it was obvious that this would not take place. The absence of DVD support for Linux prompted several programmers to attempt to create a DVD player for the open source operating system.

The events leading to the final cracking of the DVD encryption are still not completely

clear. What is obvious is that by November of 1999 there were already several applications available on the Internet that allowed people to copy a DVD by 'ripping' the contents of the disc. This was usually achieved by using a licensed player and providing it with false information about the output, instead of going to the video card drivers it would go directly to a file. All of the information available seems to indicate that by the end of 1999 an anonymous German hacker had managed to crack CSS encryption, others claim that it was an English hacker going by the unlikely name of Derek Fawcus. What is evident is that these efforts were noticed by a group of Norwegian programmers called Masters of Reverse Engineering (MoRE), headed by a 16-year-old called Jon Johansen, who has been credited by the media as the first to crack CSS. MoRE started by reverse engineering a popular DVD software player called XingDVD. To their surprise, the licensed key contained in the Xing player was not encrypted, and it allowed them to decrypt the content of any DVD. The members of the group went on to decrypt more than 170 keys by using the same encryption algorithm required to create the Xing key, this also allowed them to create a small software program called DeCSS, which could copy the contents of the disc and transfer it into a file. At the time of writing this paper, DeCSS is still widely available on the Internet.

DeCSS is not the only tool available to decrypt DVDs. Qrpff is a new program created by MIT students Keith Winstein and Marc Horowitz for a seminar on the subject. They created a small program consisting of seven lines of PERL code that is able to decrypt and play any disc by using one of the many available keys, cracked by the members of MoRE. There are other DVD rippers that are being offered via unsolicited email, with the ironic twist that you have to buy them from the pirates, but these rippers are mostly based on DeCSS technology.

DeCSS was made immediately available through various Internet locations, but as soon as those websites started receiving legal threats from the DVD manufacturers, some programmers came up with novel ways of sharing the software online. T-shirts and coffee mugs with the DeCSS code printed on them started being sold by some hacker communities. There are so many ways of encoding and hiding the code as there is imagination in the hacker as programming communities, and it can be certainly said that there is no shortage of those. Different types of hiding the code include image files, movie files, haikus, hidden text, gif files of the code, Yahoo greeting cards, etc. The possibilities are endless.

It is interesting to note that CSS has not been the only piece of DVD technology that has been cracked. There are six different DVD regions. In theory a player from one region cannot play a DVD from another region, allowing movie studios to regulate their DVD release schedule according to the film release dates in different parts of the globe. This is because movies are usually released first in the United States and Canada, and they may take up to six months to be released elsewhere. Separating the regions helps the box office success of movies that may be already available in video in the United States. As it is often the case, users did not like this arrangement, and the region protection was soon cracked.

2.3.1 Encoding and Decoding Prime Numbers

Perhaps one of the most interesting ways of sharing the DeCSS code was found by computer programmer Phil Carmody. Any computer program is a string of bits (binary digits), so every program is in the end a number. Carmody found a number which, when written into hexadecimal format, forms a gzip file. This files contains the C language code for DeCSS. The encoding would take place like this: The original DeCSS C code is compressed into a gzip file (resulting in the file Decss.gz), which is a binary representation of the original code. This file can be then converted into hexadecimal. This hexadecimal string of data can easily be converted into a decimal integer. This resulting number is a prime number. The process to decode this number would be the same, but in reverse. Take the number and input it into a hexadecimal converter (such as Hackman, or even emacs). Save the file as decss.gz, and use an uncompress utility which can read gzips. The result is the DeCSS C code, ready to be compiled. Carmody has also found a mathematical formulae that can convert this prime into an infinite number of primes. Not content with this operation, programmer Charles C. Hannum found a specific variant of the short C code which makes up DeCSS to make it directly into a prime number. The operation is to convert each of the characters in the code to their ASCII equivalent. If you view this string of digits as a single number, the result is yet another prime number.

Since these first experiments, many other programmers and mathematicians have been working to produce different prime numbers which represent the original DeCSS code. Carmody went one step further and through a long process created yet another prime number which is actually an executable representation of DeCSS, not even requiring the compilation process. Any knowledgeable enough person can simply use that prime number, convert it to hexadecimal format, and the result is the executable DeCSS program, no compilation required.

There is yet another way of performing the translating operation in an easier form, which is by the use a small perl code which retrieves the number, packs it into binary, and feeds it to gunzip, the unzip application in Linux. This produces the code as well.

The example of the encoding of DeCSS into prime numbers is just an example of the many methods available. It serves to illustrate that the determined technocratic elites that inhabit the Internet cannot be easily stopped.

3. Description of DeCSS Cases

The speed with which CSS protection was broken was not taken lightly by the movie industry, and the main studios declined to comment as soon as the news were made public by various Information Technology news outlets such as Wired and IDG. As expected, hundreds of hacker sites started making DeCSS available over the Internet as soon as the news broke out in November 1999. However, it did not take long for the movie industry to move against the creators and distributors of DeCSS. There are three main cases in the courts at the moment, both in Norway and the United States, and there are indications that there may be more suits eventually.

3.1 DVD Copy Control Assoc. v. Bunner, McLaughlin et al.

The first legal action was taken by the DVD Copy Control Association (DVD-CCA), a non-profit watchdog linked to the movie industry, whose function is to license CSS technology to hardware and software manufacturers. The DVD-CCA wrote several cease and desist letters against sites that were serving DeCSS to the Internet public, some sites complied, but others failed to do so.

In December 1999, the DVD-CCA filed a suit in a California Court against individuals who kept DeCSS software in their web pages. This complaint argued that the defendants were breaking trade secrets obtained illegally by posting the DeCSS software, which makes use of proprietary technology to avoid illegal copying of the discs. The Court issued a preliminary injunction ordering the removal of DeCSS from the defendants websites because it considered that it would be detrimental to the trade secret held by the plaintiff, but it did not go as far as to forbid linking to other sites that may have the software. The court considered that linking to other web sites was a vital part of the Internet and that it would be counterproductive to forbid site publishers to filter all sort of linking information.

The defendants appealed the injunction arguing that it violated their First Amendment rights. The California appeals court accepted this petition and eventually ruled in favour of the defendants and lifted the injunction, stating that DeCSS code is 'pure speech' that must not be subjected to prior restraint under the trade secret laws. This decision has in turn been appealed to the California Supreme Court by the DVD-CCA and it is currently under consideration.

3.2 Universal City Studios, Inc. v. Reimerdes

The second case started yet again by DVD-CCA against the online hacker magazine 2600, after repeated 'cease and desist' letters were sent by the watchdog to the magazine. As soon as DeCSS was made available to the public, 2600 placed the code on their pages, and provided links to other web sites that hosted DeCSS. When 2600 refused to take down the links and the code, nine movie studios sued the magazine and its editor, Emmanuel Goldstein, for infringement of the section 1201 of the Digital Millennium Copyright Act (DMCA), which deals with the circumvention of technology used to protect a copyrighted work. The complaint was presented to a New York Federal Court on January 14, 2000, and the case is known as Universal City Studios, Inc. v. Reimerdes. On January 20, the Court issued a preliminary injunction against 2600, which ordered that the magazine was forbidden to post DeCSS and post links to other sites that offered DeCSS to the public; the magazine accepted the order.

The case immediately was billed as a very important one regarding free speech online. It was thought that it would be a perfect battleground between the two opposing camps on the issues of fair use that are being discussed since the enactment of the DMCA, namely the copyright owners (pro) and several liberal and free speech right advocates and academics (against). As it is stated eloquently by Harvard's Openlaw site:

> ‘The case tests the scope and constitutionality of the DMCA's anticircumvention provisions -- whether the act can cripple technological innovation and scientific exploration in the name of protecting copyright. The plaintiff movie studios claim that DeCSS illegally circumvents DVD access controls, while the defense challenges the studios' assertion of an absolute right to control the manner in which movies are played, arguing that DeCSS enables fair use of DVD media and facilitates the playing of movies on unsupported operating systems. Defendants also assert that the code itself is speech that demands First Amendment protection’.

The Electronics Frontier Foundation (EFF) promptly took it upon themselves to bill 2600’s defence fund, and they had the support of several researchers and academics, which presented a large number of *amici curiae* briefs in favour of 2600. However, despite the strength of the support for the hacker magazine, in August 17 2000, the judge Lewis Kaplan ruled to maintain the preliminary injunction and to forbid 2600 to post on their website any copies of DeCCS, its code or any links to other sites hosting DeCSS.

EFF filed an appeal on behalf of 2600 appealed the decision to the Second Circuit Court of appeals on January 19 2001, arguing that the ruling went against the strict freedom of speech tests required to make a news source take down a story, and that such action went against the Constitutional guarantees of fair use of copyright. The appeals court rejected this new action and affirmed the decision against the magazine in November 28 2001.

It would have seemed that the case would have been closed with that, but because of the importance to the civil liberties camp this was not so. However, on January 14 2002 EFF requested to the entire Second Court of Appeals to reconsider the decision that denied the appeal by 2600 with an en banc petition, arguing that the ruling mistakes DeCSS for a cracking tool, dismissing its fair use purposes like allowing users of unlicensed operating systems such as Linux to view their DVDs. They also argued against the provisions against linking that both the original injunction and the appeals decision shared, stating that links are the lifeblood of the Internet. This request was also rejected by the court in June 13, 2002, closing most of their legal options but to take the case to the Supreme Court, but the 2600 magazine and EFF have announced that they will not take the case that far.

3.3 Norway v. Johansen

Besides the two cases described, there has been a very important part played by the DVD-CCA in trying to make an example of some of the people involved in the case, the most worrying example is that of the Norwegian teenager who was one of the first to crack the DVD protection.

On January 4 2000, the DVD-CCA attorneys sent a letter to the Norwegian prosecution office asking criminal charges to be brought against Jon Johansen and his father, Per Johansen. The DVD watchdog lawyers argued that Jon should be arrested for violation of Section 145 (2) of the Norwegian criminal code, which states that it is illegal to *‘break a*

security arrangement'. The letter asked for Jon's father to be indicted as well because by posting DeCSS code and links to other sites containing DeCSS they were breaking intellectual property provisions stipulated in Section 54 of the Norwegian Copyright Act, which gives copyright owners sole right to distribute their works.

Jon Johansen and his father were arrested on January 25 2000, but were later released pending an investigation into the charges by the Norwegian Economic Crime Unit (ØKOKRIM). The investigation took almost two years, and on January 9 2002 the Norwegian prosecuting unit issued charges against Jon Johansen, the case is still developing at the time of writing this paper.

It is interesting to note that Norway does not yet have provisions against anti-circumvention software; similar to what is found in the United States' DMCA. Similar provisions to those enacted by the DMCA will be implemented throughout the countries of the European Union when the Digital Copyright European Directive comes into effect . But this would not apply to Norway as it is not art of the EU. It is important to point out that due to the lack of such legislation, the Norwegian prosecutors have been forced to use legislation that is usually reserved for illegal access to computers, such as break-in hacker actions, and does not appear to be suited for the particulars of this case.

4. Legal Issues at Stake

There are several interesting legal issues brought up by the creation of DeCSS, some of them have been brought up by the cases that have been described in the previous section, but some others, perhaps the most interesting, are yet to make it to court.

4.1 DMCA Anti-circumvention

Perhaps the most obvious legal issue that has arisen from the various DeCSS cases is that of the provisions against anti-circumvention software enacted in the DMCA.
It would seem that the case against DeCSS is straightforward if we analyse the letter of the section 1201 of the DMCA. This clearly states that:

> *'No person shall circumvent a technological measure that effectively controls access to a work protected under this title*'.

The wording of this section obviously would include DeCSS and similar anti-circumvention tools used for breaking DVD protection.

The same section specifies that the Librarian of Congress will provide a set of exceptions to this rule every two years. The list was made public by the Copyright Office on October 27 2000, and includes only compilations of lists of blocked websites by filtering software applications and literary works, that fail to permit access because of a malfunction. These exemptions obviously exclude software such as DeCSS.

Seeing that the letter of the law is evidently against the existence of DeCSS, its advocates

have been forced to try to challenge the very constitutional validity of the anti-circumvention provisions found on the DMCA by implying that it goes against the constitutional protection of free speech. This was attempted more forcefully in the 2600 case. The most eloquent constitutional case can be found in the *amici curiae* presented by professors Yochai Benkler and Lawrence Lessig, both members of EFF and prominent critics of the DMCA. In their brief, the professors argue that there is a well defined separation between copyright, fair use and free speech - established many times by the US Supreme Court - which allows for several fair use provisions to exist, and that such provisions were patently challenged by the prohibitions enacted in the article 1201 of the DMCA, and specifically by technological protection such as CSS.

According to Benkler and Lessig, copyright and free speech have been separated by two landmark cases, *Harper & Row* and *Turner I.* Talking about the later in particular, they say that:

> 'Content-neutral laws that burden speech must (1) serve an important government interest (2) in a manner no more restrictive than necessary. Turner I, 512 U.S. at 662. To fulfill the first prong of the test, it must be shown 'that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.' Id., at 664.

The second prong requires that:

> 'the means chosen do not `burden substantially more speech than is necessary to further the government's legitimate interests'.

These tests are not met in their opinion by the DMCA's anti-circumvention provisions, hence their unconstitutionality. Further that, it is their argument that the DMCA imposes excessive burdens on free speech and the fair use principle.
The court dismissed these arguments by recognising the legal right of the legislative to impose restrictions on free speech in specific cases that would damage other values, in this case the trade secret of the plaintiffs .

There would appear to be a case in the arguments against the anti-circumvention protection provisions enacted by the DMCA, and it would have been interesting to see if this argument will be taken seriously by the Supreme Court, if a similar case ever makes it to that judicial body. From the reluctance to take this case to the Supreme Court by the defendants, it has become evident that EFF believes that the argument will not be listened to in the case of DeCSS. However, they have promised to take the arguments against the DMCA in other cases, possibly in others that are less straightforward than that of the 2600 magazine. It is possible that EFF has recognised that DeCSS will continue to elicit negative responses from the courts because it would seem to be related to piracy.

4.2 Freedom of Speech or Trade Secrets Case?

Although the *Reimerdes* case involving the 2600 magazine took a constitutional approach in attempting to defend the invalidity of the DMCA in regards to DeCSS, the main part of the argument from the court was centred on a negative look at the validity of the software

from the point of view of the freedom of speech elements that may be contained in it. The court found that, although it recognises that code can be considered speech, DeCSS contains a 'non-speech' element as well, which violates a legitimate interest protected by the government in legislation, such as DeCSS, and that the government can place restrictions on free speech when trying to pursue those legitimate concerns.

This view seems to be diametrically opposed to what was found by California's appellate court in the Bunner case. The court here considered whether or not this was a trade secrets case, but decided that it was not, and that the issue hindered mainly on freedom of speech.

Trade secret legislation in the US is regulated in each state by the Uniform Trade Secrets Act (UTSA). In California the act defines trade secret thus:

> 'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
> (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
> (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy'.

The UTSA expresses that a trade secret must be misappropriated by improper means if there is to be an injunction to stop the trade secret being made public. 'Improper means' are:

> '*theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means*'.

Reverse engineering is specifically not considered as misappropriation by improper means. The court found that based on this, the defendant was not involved in theft as defined by the act, and that the case should be considered as a free speech one.
In analysing the free speech value of DeCSS - and contrary to what was found in the *Reimerdes* case - California's appellate court found that DeCSS should be considered 'pure speech', and hence subject to the protection awarded by the First Amendment. The court supported this by stating that:

> 'Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSSencrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were 'compiled' to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas. (See generally Junger v. Daley, supra, 209 F.3d at pp.482483.) That the source code is capable of such compilation, however, does not destroy the expressive nature of the source code itself. Thus, we conclude that the trial court's preliminary injunction barring Bunner from disclosing DeCSS can fairly be characterized as a prohibition of

'pure' speech.'

As can be seen, both opinions are at odds with each other. It would seem that both theories cannot co-exist and it is to be desired that some sort of resolution will be forthcoming in future cases, or when the *Bunner* case makes it to the California Supreme Court.

4.3 Hyper-linking

Besides the constitutional considerations about free speech and the legality of the DMCA's anti-circumvention provisions, the courts in both *Reimerdes* and *Bunner* were asked to review the legality of posting a link to another website containing an illegal program. In the first case, the magazine 2600 was attempting to be able to link to DeCSS freely. The argument supporting the possibility of linking to DeCSS even if it was declared illegal is best expressed in the *amicus* brief presented by a number of members of the OpenLaw Internet board. In this paper, they argue that applying restrictions on hyper linking is illogical because:

> 'HTML links are simply elements in a formal citation syntax, by which one website can refer to another much as a judicial opinion or legal brief refers to its precedents. A web page with hypertext links does not 'provide' the content offered at the target pages merely by referencing those pages. Plaintiffs correctly do not seek to hold *2600* accountable for the content of linked-to pages, yet they attempt to cut the site out of the Web by denying it the ability to make references to those pages'.

The court in *Reimerdes* dismissed this argument as well by trying to argue that hyperlinks have the same speech and non-speech elements of computer programs. Luckily for the plaintiffs, the non-speech elements of the hyperlink, which are not protected by the First Amendment, happen to be present as well in those hyperlinks that connect to pages that contain DeCSS.

This solution seems not only confusing, but also reeks of an *ad hoc* argument. The argument that concedes a duality to both software and hyperlinks seems to imply that this duality will only be called upon when the court does not like the content that is being linked to. However, it would appear that the court failed to address the point made by the defendants. They are not arguing that the hyperlinks are protected by freedom of speech; they are simply arguing that the content of the sites that are being referenced on the original page is of no bearing to the referencing site. It is evident that the court missed this point entirely.

It must be pointed out that the judge on *Bunner,* specifically goes against this theory, as it allows for links to DeCSS to exist. The court found that:

> *'Links to other websites are the mainstay of the Internet and indispensable to its convenient access to the vast world of information. A website owner cannot be held responsible for all of the content of the sites to which it provides links'.*

This is certainly a more plausible and simple explanation about what hyper-linking means for the Internet. As with freedom of speech, both cases appear to be completely at odds with each other, and only future cases will help to determine which outlook should prevail.

4.4 Troublesome Prime Numbers

Although the mentioned arguments are certainly worthy of consideration, one of the most interesting cases that come out from the cracking of DVD encryption has not yet made it to the courts. This is the fact, mentioned above, that several representations of DeCSS and other DVD descramblers are being made available in several sites all over the Internet in various formats, including movies, poems, images, logos, and even prime numbers.

In the particular case of the posting of DeCSS as a prime number, all that is required for Internet users to have access to this restricted program is to know the decoding algorithm of that number into DeCSS. In Carmody's number, the algorithm is simple:

> Copy the number.
>
> Paste it into any hexadecimal translator.
>
> The resulting hexadecimal can be saved as a gzip file.
>
> Gunzip the file, which contains the C source code for DeCSS.

This algorithm is known to everybody who is knowledgeable enough in computers, and it can be even posted as the decoding instructions accompanying the number. In the strictest technical sense, posting the number would be the same as posting the DeCSS code. This can be applied to any other type of coding mechanism, such as those that are used to express DeCSS as a picture or a poem. The implications for this application of a coding algorithm can be seen throughout several pages online because restricted anti-circumvention programs can be posted in different formats online. Why then are these not being subjected to the same restrictions as the original code did? Where are the 'cease and desist' letters? Where are the suits brought against sites that carry these variations of DeCSS?

The implications of these phenomena are remarkable. In the strictest interpretation of the Section 1201 of the DMCA, the posting of these methods in any web-site could be subject to the prohibitions against anti-circumvention software that have been applied to sites which have posted links to DeCSS. In the case of the posting of DeCSS as a number, this interpretation would be very straightforward. After all, everything that is stored in a computer is simply a succession of binary bits, 0s and 1s. In other words it is all numbers, and as such, they are just expressions, which are as likely to convey meaning as code. In fact, code is nothing but numbers. One could argue that in the end, any sort of regulated content can be transferred into a number, and that such numbers, being representations in

other format of the restricted original, would have to be subject to the same restrictions. If one encodes any program that circumvents copyright protection mechanisms into a number, then it could be argued that posting the number would be as restricted as posting the code itself. The same would apply to an image that has scrambled within itself the code in some manner. The image would have to be removed from the website, as it would be just another method of promoting and transmitting the circumvention tool.

In the case of the mentioned prime numbers, this does not mean that the number itself would be protected, or that the algorithm required to encode the program that is used to circumvent the protection is protected, but that the actual posting of the number would be restricted because the number is just another representation of the offending code. This of course would be analogous to all of the other ways in which DeCSS (and other DVD scramblers) are being presented throughout different sites in whatever forms imaginable. From image files to poems, by posting any of these methods the posters are infringing the anti-circumvention provisions of the DMCA.

This example could open the door for a new way of posting executable versions of restricted material on the Internet, from text to computer cracks. This would be different from transmission of files using peer-to-peer transfers and encryption because the numbers, images, music files or poems could be posted in any website and then the user would just have to encode it into ASCII code and eventually execute it. In fact, this is happening all over the place with DeCSS. If regulators want to get rid of such practice they would have a difficult time, as the possibilities of encoding programs such as DeCSS are endless.

In the end the question remains, can the DMCA be applied to restrict the posting of numbers, images and poems that represent DeCSS code in one form or another? Would somebody dare to take this to court? This is difficult to answer. It is possible that the courts would order such methods to be taken down if they read the DMCA strictly. However, the DVD manufacturers and their watchdog group have not yet brought the many sites posting these different DeCSS representations to court to have them removed. The fact that several websites post the prime number representations of DeCSS to date is just an indication of just how widespread this method has become.

It is possible that the DVD manufacturers recognise that prosecuting the posting of prime numbers, images and other of the methods listed may be futile. For example, the conversion of a prime number into C code is not a method that any average computer user can easily manage, as it requires serious technological skill and expertise. The other reason for the reluctance of the DVD-CCA in bringing this to court may be in the fact that courts are very likely to reject the argument that the posting of a number can be restricted, even if it is a direct translation of code that is restricted by the DMCA.

It is interesting to conjecture just how a court would decide this. Given the existing rulings against DeCSS, it would not be a surprise if a court ruled that these numbers, images and even the poems be taken down, probably invoking duality of speech argument that has been used by the courts in the *Reimerdes* case. However, this will likely remain speculation for academics, a curiosity in the ever-evolving field of intellectual property

law, as it seems unlikely that the DVD owners will take these sites to court. It would seem like they are content with prosecuting only the original posters of DeCSS program in its original executable form.

4.5 Possible Implications for the UK and Europe

As it has been mentioned, it is clear that DeCSS falls into the DMCA anti-circumvention provisions, an that the legal debate in the US is now centred mostly on the issues of free speech, trade secrets and linking. The question then is open towards the application of the legal debate in the European Union.

As it was mentioned before, similar legal provisions against anti-circumvention tools will be implemented into the copyright legislations in the member states of the European Union with the coming into force of the Digital Copyright Directive. In particular, the EU requests its member states to implement legislation that:

> *'shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective'.*

The UK implementation of the Digital Directive will change the existing Copyright Designs and Patents Act of 1998. The proposed wording of the provisions read:

> '296ZB. (1) A person commits an offence if he:
> (a) makes for sale or hire, or
> (b) imports otherwise than for his private and domestic use, or
> (c) in the course of a business-
> (i) sells or lets for hire, or
> (ii) offers or exposes for sale or hire, or
> (iii) advertises for sale or hire, or
> (iv) possesses, or
> (v) distributes, or
> (d) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner any device, product or component which is primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures'.
>
> (2) A person commits an offence if he provides, promotes, advertises or markets a service in the course of a business, or otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner, the purpose of which is to enable or facilitate the circumvention of effective technological measures'.

Initially, there is no reason to think why these provisions would not apply to DeCSS, which is now hosted in various servers throughout Europe. But this initial consideration is more troublesome. The problem comes when one reads point four of that same

proposed section. This one states that:

> (4) It is a defence to any prosecution for an offence under this section for the defendant to prove that he did not know, and had no reasonable ground for believing, that:
> (a) the device, product or component; or
> (b) the services provided enabled or facilitated the circumvention of effective technological measures.

In particular, when one reads such provisions together with articles 5 and 6 of the Computer Programs Directive of 1991, this becomes more troublesome. These articles effectively allow for reverse engineering of software for the purposes of error correction and to achieve interoperability with other programs. In particular, Article 6(1) says that the program can be decompiled (which for all effects, is the same as reverse engineering) without authorisation of the owner if it is:

> '*indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs.*

If one takes into consideration that DeCSS was originally created to allow Linux users to play DVDs in their computers, one has to come to the conclusion that the cracking of DVD encryption would definitely fall into this requirement. Evidence of this is that the technology behind DeCSS is now being used by several open source and Linux developers to create Linux-based DVD players because there are no licensed players for this operating system. This opens many questions about the survival of DeCSS in Europe. One could certainly make a strong argument that in Europe DeCSS will be less likely to be attacked than in the United States.

Another interesting issue to consider in regards to DeCSS in Europe are the questions about hyperlinks to anti-circumvention programs. Although the debate seems to be still open in the United States in this regard, it is interesting to try to see if similar problems would apply in Europe. Surprisingly, the problem of linking to a page that is infringing copyright has not been brought to court extensively. The main case that exist did not produce a ruling, and it is that of *Nottinghamshire County Council v. Gwatkin and others*, the Nottinghamshire Council published a report in 1990 about an alleged case of child abuse by social workers. In 1997 a web site called 'The Broxtowe Files' copied the report and placed it on the Internet. The Council requested the text to be removed, which the site administrators did. However, the site maintained links to mirror pages in Belgium and the United States that contained the report. The council filed an injunction to get these links removed, but later withdrew its complaint, unfortunately not producing a ruling for this case. It will be interesting to see how the courts rule one of these issues.

A more successful route to attempt to stop DeCSS in the EU would be to hold websites holding these links liable. There is a precedent for this in Germany; the Bavarian State Court ruled that AOL was to be held liable for music being illegally swapped through that network. Although this ruling does not refer to linking, it could definitely be argued that if an ISP is to be held liable for the illegal interactions of its members, a web page could

be similarly held liable for the links that lead to infringing copyright materials. A similar analogy could possibly be applied to recent cases across Europe where the courts have ruled against websites that provide links to data that has been extracted from a protected database in accordance to the Database Directive.

It would seem that most of the questions are still open because of lack of treatment of these issues in the courts. It may be interesting to see if the DVD manufacturers will attempt to attack the European sites which hold and link to DeCSS, and if this takes place, how will courts decide.

5. Conclusion

The ferocity and swiftness with which the movie industry has attacked the creators and distributors of DeCSS is not an isolated incident. There seems to be a willingness among copyright owners to launch into pre-emptive legal strikes against any perceived offence.

There appears to be growing room for concern among academics, users and consumers about this trend. There are very worrying cases, such as that of the Russian hacker Dmitry Sklyarov, who cracked the copy protection in the Adobe software used to read e-books. Ed Felten, a Princeton researcher and academic who was forced to withdraw a paper that discussed the vulnerability of another method of protection, the Secure Digital Music Initiative (SDMI), has also faced the grinding power of the copyright owners flexing their muscles. The copyright industries are constantly lobbying for stricter legislation, and in most cases, obtaining it. The DMCA, the European Digital Copyright Directive, and the Database Directive are just some examples of this trend.

In the case of DeCSS, the reaction by the industry seems excessive. It could be said that DVD manufacturers are trying to make a public example of some of these users. There is a genuine case to be made by those who advocate the cracking of the DVD encryption with the purpose of viewing DVDs in the Linux operating system. This could definitely be considered fair usage of a purchased copyrighted work in a universe where copyright protection has not gone mad. Another fact that is constantly forgotten by the courts and the DVD manufacturers is that DVDs contain too much information to be able to be copied easily, and certainly not by means of DeCSS, which produces raw output of the file. An average DVD contains from 4.5 to 8 gigabytes of information, the equivalent of 7 to 14 normal CDs. Such an amount of information cannot be transferred through the Internet at normal speeds, and it is not even viable using high bandwidth connections. DVD piracy exists, but it uses other methods such as drive imaging, not through DeCSS. The industry is not requesting imaging programs such as Norton Utilities, Norton Ghost or Drive Imager to be declared illegal. Questions must be asked as to what sort of double standards are at work; it is entirely feasible that what the movie industry is making is simply looking for victims to hang in the virtual town centre to set an example for the rest of the hacker community.

Notes and References

With thanks to Marian Szczepkowski, John Sullivan and Mark R. Jenkins for their invaluable suggestions.

Table of Cases

Bookmaker's Afternoon Greyhound Services Ltd. V Will Gilbert (Staffordshire) Ltd. [1981] 3 All ER 241.

DVD Copy Control Assoc. v. McLaughlin, Bunner et al. Cal. Super. Ct., Santa Clara Cty., CV-786804.

Harper & Row, 471 U.S. at 560.

Microsense Systems Ltd. V Control Systems Technology Ltd. 17 June 1991, Chancery Division.

Nottinghamshire County Council v. Gwatkin and others (High Court of Justice, Chancery Division, June 3, 1997). Not reported.

Pavlovich v. Superior Court of Santa Clara County, Cal. App. Ct., No. H021961, 8/7/01

Turner I, 512 U.S. at 662.

Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

Bibliography

- (2001), 'DVD Frequently Asked Questions (and Answers)'. *DVD Demystified*, October 6, 2001 <<http://www.dvddemystified.com/dvdfaq.html>>.

- (2001), 'Digital Versatile Disc'. *Whatis?com,* July 25, 2001 <<http://whatis.techtarget.com/definition/0,,sid9_gci213923,00.html>>.

- (2001), 'True Stories: Prime Suspect', Linux User, Issue 10 - May 2001 <<http://www.linuxuser.co.uk/articles/issue10/lu10-True_stories-Prime_suspect.pdf>>.

- (1998), 'What is Encryption?', *In BBC News*, February 20, 1998 <http://news6.thdo.bbc.co.uk/hi/english/special_report/1999/03/99/economy/newsid_57000/57866.stm <http://news6.thdo.bbc.co.uk/hi/english/special_report/1999/03/99/e-conomy/newsid_57000/57866.stm>>

- (2001), 'German Court Upholds Ruling Against AOL', *The Nando Times*, March 9, 2001 <http://archive.nandotimes.com/technology/story/0,1643,500461705-500703847503843955O,00.html <http://archive.nandotimes.com/technology/story/0,1643,500461705-500703847-503843955-0,00.html>>.

2600 Quarterly (2000), *Father and Son Arrested,* January 25, 2000 <<http://www.2600.com/news/display.shtml?id=343>>.

2600 Quarterly (2001), *DVD Lawsuit Archive*, 2001 <<http://www.2600.com/dvd/>>.

Bainbridge, D (1999), *Intellectual Property*, Fourth Edition, London, Pitman Publishing.

Benkler, Y and Lessig, L (2001), *Brief of Amici Curiae in Support of Appellant, Jan. 26, 2001, Universal v. Reimerdes*. January 26, 2001 <<http://www.eff.org/IP/Video/MPAA_DVD_cases/20010126_ny_2profs_amicus.html>>.

Bing, J (2000), *A Legal Perspective on the Norwegian DeCSS Case*, 25 January 2000 <<http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20000125_bing_johansen_case_summary.html>>.

Caldwell, C (2002), 'Illegal Prime', *The Prime Glossary*, <<http://primes.utm.edu/glossary/page.php/Illegal.html>>.

Case Comment (2001a),'United States: Injunction Against Posting of DeCSS Affirmed; DMCA Held Constitutional', *World E-Commerce & IP Report*, 1(15), pp.9-10.

Case Comment (2001b),'United States: Injunction Barring Web Posting of DECSS is Unconstitutional Prior Restraint on Speech', *World Internet Law Report*, 2(12), pp.28-29.

Case Comment (2002), 'United States: Injunction Against Posting of DECSS Affirmed', *World Internet Law Report*, 3(1), pp.23-24.

Costello, S (2001), 'Seven lines of code can crack DVD encryption', *CNN-IDG*, March 13, 2001 <<http://asia.cnn.com/2001/TECH/internet/03/12/DVD.code.idg/>>.

D'Ambrise, R (1997), *A Closer Look at DVD,* <<http://www.cd-info.com/CDIC/Technology/DVD/dvd.html>>.

DeCSS Central. *CSS and DeCSS* <<http://www.lemuria.org/DeCSS/decss.html>>.

Downing, R (2001),'US: Illegal Copying of DVDs', *Practical Law Companies* (PLC) 12 (9), p.5.

Electronic Frontiers Foundation (2000), *Letter from US DVD-CCA's Attorney to Norway Prosecutor*. January 4, 2000. <<http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20000104_dvdcca_no_prosecutor_letter.en.html>>.

Electronic Frontiers Foundation (2001), *Publisher Appeals Injunction Against News Story*. 19 January 2001. <<http://cryptome.org/eff011901.htm>>.

Electronic Frontiers Foundation (2002a), *Norway Indicts Teen Who Published Code Liberating DVDs,* January 10, 2002. <<http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20020110_eff_pr.html>>.

Electronic Frontiers Foundation (2002b), *2600 Magazine 2nd Cir. En Banc Appeal*. Jan 14, 2002: <<http://www.eff.org/IP/Video/MPAA_DVD_cases/20020114_ny_2600_appeal.html>>.

Council of Europe. *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society,* Official Journal L 167, 22/06/2001. Article 6 (1). <<http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&model=guichett>>

Evers, J (1999), 'E-commerce encryption now vulnerable?' *CNN Interactive*, August 30, 1999. <http://www.cnn.co.uk/TECH/computing/9908/30/ecommun.safe.idg/index.html>.

Fraunhofer Institut (1999), *MPEG Audio Layer-3*. 1999. <http://www.iis.fhg.de/amm/techinf/layer3/index.html>.

Froomkin, D (1998), 'Deciphering Encryption', *Washington Post Online*, May 8, 1998. <http://www.washingtonpost.com/wpsrv/politics/special/encryption/encryption.htm <http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm>>.

Gailly, J P (1999), *comp.compression Frequently Asked Questions*. September 5, 1999 <<http://www.faqs.org/faqs/compression-faq/part1/>>.

Greene, T (2001),'World's First DeCSS Executable Prime Number', *The Register*, September 11, 2001 <<http://www.theregister.co.uk/content/6/21591.html>>.

Kaplan, C S (2000), 'DVD Case Will Test Reach of Digital Copyright Law', *Cyber Law Journal Weekly*, July 14, 2000. <<http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/14law.html>> .

Kelly, J S (2000), 'Interview with Jon Johansen', *Linux World*, January 2000 <<http://www.linuxworld.com/linuxworld/lw-2000-01/lw-01-dvd-interview.html>>.

Kesden, G (2000), *Content Scrambling System,* December 6, 2000 <<http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/index.html>>.

King, D (2001), *DVD Video Ten Times More Popular than CD,* 22 January 2001 <<http://www.bva.org.uk/press_release/dvd/dvd_220101.html>>.

Levy, S (2001), *Crypto: Secrecy & Privacy in the New Code War,* London, Penguin Books.

Movies UK. *DVD Regions* <<http://www.moviesuk.fsnet.co.uk/dvd_regions.htm>>.

Moving Picture Experts Group, *About MPEG*, September 1998 <http://www.cselt.stet.it/mpeg/about_mpeg.htm> .

Parker, D (1999), 'Cease and DeCSS: DVD's Encryption Code Cracked', *Emedia Industry News*, November 4, 1999 <http://www.zepa.net/hypermail/elug/1999/11/0039.html <http://www.emediapro.net/news99/news111.html>>.

Patrizio, A (1999a), 'DVD's Fragmented Future', *Wired News*, August 30, 1999 <<http://www.wired.com/news/technology/0,1282,21497,00.html>>.

Patrizio, A (1999b), 'DVD Piracy: It Can Be Done', *Wired News*, November 1, 1999. <<http://www.wired.com/news/digiwood/0,1412,32249,00.html>>.

Patrizio, A (1999c), 'Why the DVD Hack Was a Cinch', *Wired News*, November 2, 1999 <<http://www.wired.com/news/technology/0,1282,32263,00.html>>.

Pearson, H E (2000), 'Open Source: The Death of Proprietary Systems?' *Computer Law & Security Report* (CLSR), 16(3), pp.151-156.

Seltzer, W (2002), 'Openlaw DVD Roadmap', *Berkman Center's Openlaw* <<http://eon.law.harvard.edu/openlaw/DVD/roadmap.html>>.

SirMontego (2000), 'DVD Regions Explained', *Epinions*, April 26 2000 <<http://www.epinions.com/elec-review-665C-105932C-39077F49-prod6>>.

Suthersanen, U (2001/02) 'Napster, DVD and All That: Developing a Coherent Copyright Grid for Internet Entertainment', *Yearbook of Copyright & Media Law* (YC & ML), 6, 207-250.

Thomas, A (2000), 'DVD Encryption: DeCSS', *Entertainment Law Review* (Ent. LR), 11 (6), pp.135-137.

Touretzky, D S (2000a), Gallery of CSS Descramblers. <<http://www.cs.cmu.edu/~dst/DeCSS/Gallery>>.

Touretzky, D S (2000b), *Source vs. Object Code: A False Dichotomy*. July 25, 2000. <<http://www-2.cs.cmu.edu/~dst/DeCSS/object-code.txt>>

UK Patents Office (2002), *Draft Amendments to the 1988 Act covering the main changes proposed to implement Directive 2001/29/EC*. August 13, 2002. <<http://www.patent.gov.uk/about/consultations/eccopyright/annexa.htm>>

US Copyright Office (2000), *Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works.* October 28, 2000 <<http://www.loc.gov/copyright/1201/anticirc.html>>.

Vitaliano, F (1997), 'DVD, The Bad, The Ugly, and The Digital Pits', *21st Impact*, 1997 <<http://www.vxm.com/21R.91.html>>.

Wallace, J, Mangan, M (1997), *Sex, Laws and Cyberspace*, New York, 1st Owl Books, 1997.

Appendix

This prime number can be turned into DeCSS:

48565078965739782930984189469428613770744208735135792401965207366869851340104723744696879743992611751097377770102744752804905883138403754970998790965395522701171215702597466699324022683459661960603485174249773584685188556745702571254749996482194184655710084119086259716947970799152004866709 9

759235960613207259737979936188606316914473588300245336972781813914797955513399949394882899846917836100182597890103160196183503434489568705384520853804584241565482488933380474758711283395989685223254460840897111977127694120795862440547161321005006459820176961771809478113622002723448272249323259547234688002927776497906148129840428345720146348968547169082354737835661972186224969431622716663939055430241564732924855248991225739466548627140482117138124388217717602984125524464744505583462814488335631902725319590439283873764073916891257924055015620889787163375999107887084908159097548019285768451988596305323823490558092032999603234471140776019847163531161713078576084862236370283570104961259568184678596533310077017991614674472549272833486916000647585917462781212690073518309241530106302893295665843662000800476778967984382090797619859493646309380586336721469695975027968771205724996666980561453382074120315933770309949152746918356593762102220068126798273445760938020304479122774980917955938387121000588766689258448700470772552497060444652127130404321182610103591186476662963858495087448497373476861420880529443

This is the Perl script which automates the process:

```
#!/usr/bin/perl

# Public domain. Questions to Jamie McCarthy, jamie@mccarthy.vg

 use LWP::Simple;

 use Math::BigInt;

 my $html = get
(‘http://www.utm.edu/research/primes/curios/48565...29443.html’);

 my($prime) = $html =~ m{<blockquote>([^<]+)</blockquote>};

 $prime =~ tr{0-9}{}cd;

$prime = Math::BigInt->new($prime);

 my $binary = '';

while ($prime > 0)

  {

 $binary = pack(‘N’, ($prime % 2**32)) . $binary;

 $prime /= 2**32;

  }

 $binary =~ s{^\0+}{};

 local *FH;

 open(FH, ‘| gunzip -acq’) or die ‘cannot gunzip, $!’;
```

```
binmode FH;
print FH $binary;
close FH.
```