5 Lecture 5: Microsoft's Favorite Elliptic Curve

This lecture concerns an application of elliptic curves over finite fields to cryptography. Our central example involves "version 2 of the Microsoft Digital Rights Management (MS-DRM) system", as applied to `.wma` audio files.

I learned about this protocol from an anonymous paper by the clever hacker "Beale Screamer" who broke MS-DRM.

5.1 Media Background

"December 2001

Not surprisingly, Microsoft's digital rights management scheme was cracked in mid-October. It's not surprising because, well, it's Microsoft, ever the target of those looking to test the strength of a 900-pound gorilla. Specifically, version 2 of Microsoft's DRM was compromised, with special attention given to audio files. The code was cracked by "Beale Screamer," an alias inspired by Howard Beale in the movie Network who proclaimed "I'm mad as hell, and I'm not going to take this anymore!" Screamer also provides a DOS utility that strips away Microsoft's DRM protection of audio files. Interestingly, there is no code, "either real code or pseudo-code," contained in the accompanying documentation. According to Screamer, "All that's in this document is a straight mathematical discussion, which should be fully protected under the 1st Amendment to the U.S. Constitution." You may recall the DeCSS case where computer "code" was not given the same First Amendment rights as straight English text, thereby forcing those who wish to publish their cracks to disguise source code in plain English. Beale Screamer is apparently angry that he/she, under Microsoft's DRM protection, can't make copies of purchased audio files for playback on other devices. [...]"

- EContent Magazine

Microsoft attempts to silence Screamer

By James Middleton, vnunet.com [23-10-2001]

Microsoft is apparently examining its legal options after an as yet unidentified hacker last week managed to compromise its Digital Rights Management (DRM) anti-piracy technology, and post the results on the internet.

The technology is one of the many copy protection systems currently being bandied about by software vendors to prevent audio file piracy.

But a hacker known only as Beale Screamer managed to create a utility capable of bypassing the protection system known as FreeMe. Now the program is being widely circulated on the net.

According to Microsoft, over 275 companies have licensed the DRM technology as a protected system for distributing audio and video. The company said it is now working with its partners to minimise the risk posed by the hacker tool.

But it is thought Microsoft is still at a loss as to the coder's identity, even though it is looking to the Digital Millennium Copyright Act (DMCA) to take legal action against the hacker.

5.2 Microsoft's Favorite Elliptic Curve

The elliptic curve used in MS-DRM is an elliptic curve over the finite field $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ of integers modulo p, where

$$p = 785963102379428822376694789446897396207498568951.$$

Beale Screamer remarks that this modulus has *high nerd appeal* because in hexadecimal it is

$$89\mathrm{ABCDEF}012345672718281831415926141424\mathrm{F}7,$$

which includes counting in hexadecimal, and digits of e, π, and $\sqrt{2}$. Microsoft's favorite elliptic curve E is

$$\begin{aligned} y^2 = x^3 &+ 317689081251325503476317476413827693272746955927x \\ &+ 79052896607878758718120572025718535432100651934. \end{aligned}$$

The group $E(\mathbb{F}_p)$ is cyclic of order

$$\#E(\mathbb{F}_p) = 785963102379428822376693024881714957612686157429,$$

and is generated by

$$\begin{aligned} B = (&771507216262649826170648268565579889907769254176, \\ &390157510246556628525279459266514995562533196655). \end{aligned}$$

5.3 Nikita and Michael

Our heros Nikita and Michael love to share digital music  when they aren't too busy thwarting terrorists. When Nikita installed Microsoft's content rights management software on her compute, it sneakily generated a private key

$$n = 670805031139910513517527207693060456300217054473,$$

which it stealthily hid in bits and pieces of various system files. In order for Nikita to play Juno Reactor's latest hit `juno.wma`, her web browser contacts a Microsoft rights management partner. After Nikita gives Microsoft her credit card number, she is allowed to download a license to play `juno.wma`. Microsoft created the license using the ElGamal public-key cryptosystem (see below) in the group $E(\mathbb{F}_p)$. Nikita's license file can now be used to unlock `juno.wma`, but *only* on Nikita's computer. When she shares both `juno.wma` and the license file with Michael, he is very annoyed because he can't play `juno.wma`. This is because Michael's computer doesn't know Nikita's computer's private key (that integer n above), so Michael's computer can't decrypt the license file.

`juno.wma`

5.4 The Elliptic Curve Discrete Logarithm Problem

Definition 5.1. If E is an elliptic curve over $\mathbb{F}_p$ and B is a point on E, then the *discrete log problem* on E to the base B is the following problem: given a point $P \in E$, find an integer n such that $nB = P$, if such an integer exists.

For example, let E be the elliptic curve given by $y^2 = x^3 + x + 1$ over the field $\mathbb{F}_7$. We have

$$E(\mathbb{F}_7) = \{\mathcal{O}, (2,2), (0,1), (0,6), (2,5)\}.$$

If $B = (2,2)$ and $P = (0,6)$, then $3B = P$, so $n = 3$ is a solution to the discrete logarithm problem.

To the best of my knowledge, the discrete logarithm problem on elliptic curves when p is large is *really hard* unless $\#E(\mathbb{F}_p)$ is "smooth", i.e., a product of small primes, or E is "supersingular" in the sense that $p \mid \#E(\mathbb{F}_p)$. The Microsoft curve has neither of these deficiencies, and I expect that the discrete logarithm on that curve is quite difficult. This is not the weakness that "Beale Screamer" exploits in breaking MS-DRM.

5.5 ElGamal

How can we set up a cryptosystem using an elliptic curve? There is an analogue of Diffie-Hellman on elliptic curves, but that's not what Microsoft uses. Instead, they use the ElGamal cryptosystem.

Nikita would like anyone to be able to send her encrypted messages using the ElGamal protocol. First she computes and tells everyone the following information:

1. a prime number p,
2. an elliptic curve E over $\mathbb{F}_p$, and
3. a point B on E.

She then chooses a random integer n, which is kept secret, and computes and publishes nB.

Suppose Michael would like to send a message P to Nikita. He computes a random integer r and sends the pair of points $(rB, P+r(nB))$. To read the message, Nikita multiplies rB by her secret key n to get $n(rB) = r(nB)$, and subtracts this from the second point to get

$$P = P + r(nB) - r(nB),$$

thus decrypting the message.

Exercise 5.2. Note that ElGamal makes sense in any abelian group where the discrete logarithm problem is difficult. For example, let p be a prime and consider the abelian group C of numbers modulo p that are coprime to p. Create an example that illustrates ElGamal in C.

The following example is based on an example taken from Beale Screamer's paper.

Example 5.3. Nikita's license files contains the pair of points $(rB, P+r(nB))$, where

$$rB = (179671003218315746385026655733086044982194424660,\ 697834385359686368249301282675141830935176314718)$$

and

$$P + r(nB) = (137851038548264467372645158093004000343639118915,\ 110848589228676224057229230223580815024224875699).$$

Nikita's computer sneakily loads the secret key

$$n = 670805031139910513517527207693060456300217054473$$

into memory and computes

$$n(rB) = r(nB) = (328901393518732637577115650601768681044040715701,\ 586947838087815993601350565488788846203887988162).$$

It then subtracts this from $P + r(nB)$ to get

$$P = (14489646124220757767,\ 669337780373284096274895136618194604469696830074).$$

That x coordinate, 14489646124220757767, is the top secret magic "content key" that unlocks `juno.wma`.

If Nikita knew the private key n that her computer generated, she could compute P herself and unlock `juno.wma` and share her music with Michael, just like she used to share her favorite CDs with Michael. Beale Screamer found a weakness in Microsoft's system that let him find n. **Out of fear of the DMCA and Microsoft, I won't tell you any details**, but you can find them easily enough online.

Microsoft has undertaken a difficult and interesting problem. *How can Microsoft store data on Nikita's computer in such a way that Nikita cannot access it, but Nikita's computer can?* I don't know the answer.

5.6 Why Elliptic Curves?

There are several advantages to using elliptic curves (instead of $\mathbb{F}_p$) for cryptography. Elliptic curve cryptosystems with smaller key sizes "appear" to be as secure as "classical" $\mathbb{F}_p$ cryptosystems with much larger key sizes. My understanding is that the existence of a fast algorithms for factoring integers would not, as far as we know, automatically break elliptic curve cryptosystems.

Some mobile phones also use elliptic curve cryptography. Do you have an elliptic curve in your pocket right now?