Adam Winebarger
13 Fed 2022
Cryptography & Privacy

Automathography

"It's my opinion that Adam should retake highschool Algebra next year" was a defining sentence for my sordid history with mathematics. It has been almost two decades since the first time I took highschool algebra; and while I can no longer remember the name of the teacher I had for that class, I can still vividly remember my disdain for it. Frankly, it probably shouldn't have carried as much weight as it did. I was in 8th grade at the time, so repeating it would have put me on par with most of the other students in my grade; and I knew the material: my C grade in that class was due in large part to the fact that I didn't like to show my work when answering questions. But that ended up being the beginning of my dislike for mathematics in high school. Even going into high school mathematics, I still didn't see much of a point to showing my work. Retaking Algebra 1 was, unsurprisingly, a breeze and I realized that if I wrote random numbers and symbols with a correct answer, then I got full credit on a problem more often than not. Back then, I thought that I wasn't a fan of mathematics. But looking at it in retrospect, I can say that I just wasn't a fan of the people teaching it.

Given how long it has been since my Middle-School/High School Algebra 1 days, I'm not really sure anymore at what point I started to like mathematics. Maybe it was taking Algebra II with my Track & Field coach as the teacher. Or perhaps it was my Senior year when I took Physics and Personal Finance and I finally got to see some mathematical concepts come to life. But I felt like I had a pretty good grasp on a lot of the mathematical concepts by the end of High School, despite my grades saying otherwise. While I don't remember exactly what my final GPA was for high school, I'm reasonably certain that it was somewhere in the 2.4-2.7 range. Frankly, I didn't care much about academics at that point. At 17, I had decided that I was joining the Army and I figured little-to-none of what I had learned up until that point would come in handy going forward. I was wrong.

In the army, the official title for my Military Occupational Specialty (MOS) was *Fire Support Specialist*. I dealt primarily with coordination of indirect assets (such as Artillery and Air Strikes) and what I thought had been useless skills largely ended up coming in handy. Unit-conversion was something that had to be used fairly regularly as most everything done in the Army is metric, but the Air Force still liked to use feet for certain things. Similarly, most of the Army used degrees to determine direction while Artillerymen would use a unit of measurement called mils (1 degree = 17.777… mils) and converting back and forth between the two was something that people in my job

had to do on the regular. Flash-to-bang was used to determine the distance of an impacted round by counting the seconds between seeing the impact and hearing it, then multiplying by 350 (actual speed of sound is 343, but rounding was often done in order to get calculations in a timely manner). An observer-target factor was also used to make deviation-corrections in round impacts at greater distances as a round landing 30 meters “to the right” at 1 Km out will look similar to a round landing 60 meters to the right at 2 Km. Suffice it to say, the math I had learned in high school turned out to not to be useless during my time in the army.

After getting out of the army, I enrolled at Grand Rapids Community College. As part of enrollment, new prospective students are required to take an aptitude test in mathematics to see where students are. Despite the fact that I was seeing a lot of Algebraic concepts for the first time in 6 years, I did quite well and my advisor recommended that I start in pre-calc. Even so, I felt that it would be best to err on the side of caution and begin with college Algebra. It seemed as though everything was going swimmingly until it came time to take pre-calc with Professor Hadley.

Now Prof. Hadley had what I’ve come to refer to as “the plight of the subject-matter expert”. It wasn’t my first time seeing this in a college environment. In fact, I have been met with “What do you mean you don’t understand x? It’s x” by many computer science professors when voicing to them my lack of understanding of a certain problem or concept. But prof. Hadley took this to a whole other level. Every lecture of his began with him teaching the lecture material, then either saying “This isn’t how you would do this in real life” and simultaneously teaching us the way to do it for the class and the way to do it in real life with little-to-no warning when he was switching between the two; or going off on a random tangent about something that may or may not have been related (the most memorable one was how wind-tunnel testing at General Motors differs from other auto-manufacturers). While I struggled, I knew I wasn’t the only one struggling. This was made especially apparent by the fact that he let us take our third exam as a class (meaning we could use notes, the book, our phones, and each other).

While I have not met any professors quite like Prof. Hadley since transferring to GVSU, there are certainly a few who tend to graze over certain important bits of information when teaching how to solve various mathematical problems. I think that younger me tended to place the blame more on math itself for those types of issues rather than the individuals teaching it. For now, I don’t know if I would say that I like math, but I certainly see the usefulness of it. It is a tool: a means to an end, and essential for a lot of what I do as a computer science major. However, as a Computer Science major, I definitely feel more inclined to build algorithms to handle complex mathematical operations for me rather than do them myself.

Update:

Very little has changed since the initial writing of this auto-mathography. While no major breakthroughs have been made over the course of this semester, it has been a great experience in honing my craft when it comes to the programmatic implementation of various mathematical concepts. Functional notes, a concept I had worked on when working in applied statistics to demonstrate concepts using various C++ classes, proved to be very worthwhile over the course of this cryptography class. The only major issue that was had was in the early part of the semester when I was not putting the C++ code into classes (recycling common function names like “encode” and “decode” was leading to some redeclaration issues). However, upon revisiting my C++ functional notes and doing some rewrites with functions existing within classes made my C++ functional notes being incredibly helpful over the course of this… course.

While none of these ciphers were particularly news to me - about a third of Intro to Cybersecurity was a section covering various cryptographic ciphers - implementing them programmatically presented some interesting challenges. Particularly with any ciphers involving tables - ADFGVX was particularly troublesome - figuring out how to “swap” values made for a pretty unique challenge. Even things that should have been simple - like my AES encryptor - provided some unique challenges when they were implemented in different contexts. In the case of encrypting and decrypting with AES. Converting from a byte array to a string was leading to some degradation issues. In any case, it was a very good lesson in how changes may need to be made based on the implementation of a program - even if it’s built with portability in mind. But this hardly pertains to mathematics.