Cryptography 4/3

Reagan Shirk

April 3, 2020

Lattice

- Integral linear combination comes into play somewhere, the points of the vectors V and W $((v_1, v_2), (w_1, w_2))$ can be written as linear combinations of each other, where you have a matrix A that represents the base change
  - It's been two years since I've taken linear algebra so I'm hoping that I'm using all of this vocab right, my memory is a little foggy
  - The determinant of A is 1 and $A \in \mathbb{Z}^{2\times 2}$
- w_2 is the most important thing for us because it's the shortest vector (still nonzero though, I don't really know why that needs to be specified but I guess it does)
- Alrighty he's lost me. There's a big ass matrix on the screen though
- T is the solution for subset sum, whatever that means
  - $x_i = 1$ if $m_i \in T, 0$ otherwise, I also don't know what this is talking about
- Guys I don't even know why I'm taking notes, I'm not paying attention
  - This subject is so interesting but I hate this class because I never know what Cheng is talking about

LLL-BK$\mathbb{Z}$

- Lenstra-Lenstra-Lovasz
  - The two Lenstra's are brothers
- Apparently this is an important algorithm
- It's an approximation algorithm which means that it can't find the shortest vector, but it can approximate the shortest vector
- There is an approximation factor of 2^n
  - LLL algorithm: $|V_1| \leq 2^n \lambda_1$
  - 2^n is too large