Cryptopgraphy 4/1

Reagan Shirk

March 31, 2020

Meet in the Middle Algorithm

$$M = \{a_1, a_2, \cdots, a_n\} T \subseteq M \text{ such that } \Sigma_{x \in T}\ (x) = S$$

- Naive algorithm: try all of the subsets
  - $\tilde{O}(2^n)$ time complexity
- The Meet in the Middle Algorithm improves the naive algorithm
  - He's totally lost me, I'm gonna look this up on GeeksforGeeks and hopefully I'll remember to update my notes with what they say
  - Somehow, we end up knowing that the complexity is:

    $$\tilde{O}(2^{\frac{n}{2}})$$

  - I don't really know what the stuff below is about but it somehow pertains to this algorithm, something about the subsets for each half of...something?

$$M = M_1 \cup M_2 M_1 = \{a_1 \cdots a_{\frac{n}{2}}\} M_2 = \{a_{\frac{n}{2}+1} \cdots a_n\}$$

- Proposition 7.3 from the book:
  - If we need 80-bit security for Merkle-Hellman, then we need $n \geq 160$

Lattice

- Suppose we have two linearly independent vectors over the real numbers
  - We know that $v_1\mathbb{R} + v_2\mathbb{R}$ will give us the whole plane
  - Moving into number theory, we want to move away from $\mathbb{R}$
- Now we have two linearly independent vectors over $\mathbb{Z}$
  - We know that $v_1\mathbb{Z} + v_2\mathbb{Z}$ gives us a lattice
- Lattice definition: given n linearly independent vectors $\in \mathbb{R}^m$ where $n \leq m$, the lattice generated by them is the set of vectors

  $$(b_1, \cdots, b_n) = \{\Sigma_{i=1}^n (x_i b_i) : x_i \in \mathbb{Z}\}$$

  where the vectors $b_1, \cdots, b_n$ form a basis of the lattice
- The determinant of a lattice is the area/volume (dependent on the number of dimensions) of the fundamental domain
  - The fundamental domain is really simple but I'm struggling to describe it in words, so if you're reading this remind me to think about it and update my notes