Shannon's Theory

Math 4175

§3.1. Computational Security

We have studied various cryptosystems in previous Chapter. Now we would like to know the security of these systems with respect to certain specific type of attacks. So we first consider three approaches to evaluating the security of a cryptosystems.

1. Computational security: A cryptosystem is said to be computationally secure, if the best algorithm for breaking this system requires at least N operations, where N is a very large pre-determined number.

- The computational power and speed of the computers are steadily getting better and better. So a cryptosystem that is computationally secure now, might not be secure in the near future.
- Also, computational security against one type of attack does not guarantee security against another type of attack.

§3.1. Provable Security

2. Provable Security: A cryptosystem is said to be provably secure, if it cannot be broken unless a well-studied difficult problem is solved.

- This approach again does not provide absolute security. It only provides the evidence of security relative to another problem (such as whether the given large number N is a prime number or a problem is NP-complete.
- Like in the previous case, as our ability to solve the difficult problems improves, this security may fade away in future.

§3.1. Unconditional Security

3. Unconditional Security: A cryptosystem is defined to be unconditionally secure, if it cannot be broken even with infinite computational resources.

In this chapter, we will develop a theory to verify whether certain cryptosystems are unconditionally secure against cipher text only attack. We will discuss several of Claude Shanon's idea published in his 1949 paper titled Communication Theory of Secrecy Systems in Bell Systems Technical Journal.

§3.1. Unconditional Security

- For example, we learned in previous chapter that Shift Cipher, Substitution Cipher and Vigenère Cipher are NOT computationally secure against cipher text only attack if a sufficiently large cipher text is given.
- We will prove that both Shift Cipher and Substitution Cipher are unconditionally secure if a single element of plaintext is encrypted with a given key.
- Similarly, Vigenère Cipher with key word length m is unconditionally secure, if only a string of m alphabetic characters are encrypted by using this key.

In order to study the unconditional security, we need to review probability theory.