POIS: Impossible Problems, Imperfect Solutions

Atreyee

January 14, 2019

> *All information security problems have a common feature, which is that they are impossible to solve perfectly.*
>
> *All information security problems have a common solution and that is the use of destructive interference of impossibilities.*
>
> *Therefore, this course is truly fundamental and should be named The Science Of The Impossible.*
>
> - Prof. Kannan Srinathan

1 Principles of Security

1.1 Kirchoff's Principle of Security

Security is derived from the secrecy of the encryption key, not from the obscurity of the encryption algorithm.

Thus, an ideal hashing algorithm should be non-invertible.

1.2 Principle of Sufficiently Large Keyspace

2 Ciphers

2.1 Definition

2.2 Monoalphabetic Substitution Cipher

How to break: frequency attack

2.3 Vigeneve Cipher

How to break: TODO

3 The Secrets of Secrecy

3.1 Heuristic Secrecy

3.2 Provable Secrecy

3.3 Proven Secrecy

3.4 Shannon's Perfect Secrecy

4 The Perfect Magical Cipher: Vernam's Cipher

Theorem 1. *One Time Pad is perfectly secret.*

Proof. TODO: FIND PROOF □

5 We Need More Keys

Theorem 2. *The condition of perfect secrecy is that the keyspace should be larger than or equal to the message space.*

Proof. TODO: GET PROOF □

6 Channeling Secrecy

Theorem 3. *Transmission of a perfectly secure message can only be done at the rate of the secure channel.*

Proof. TODO: GET PROOF □