Theorem
Meta

Theorem: Secure Communication is impossible. Proof: Shannon Theory

(Impossibility proofs are different from & harder than possibility proofs)

Definitions of security needs to be known to prove impossibility.

Kerckhoff's Principle: Security of a system should be due to secrecy of key & not obscurity of algorithm used

(Fallability of security through obscurity)

Kerckhoff's argument: Not revealing $\neq$ will never be found out

→ can be reverse engineered by human or machine

→ f is a part of the password (key)

$f(x) = U(f, x)$: f itself has to be stored securely · suboptimal use of secure memory

→ Need different algorithms for communication with each actor - does not scale

→ Redeeming virus is hard - like reset password

Why Kirchhoffs Principle is mandatory:

→ Standardization

Ex: Internet: http, https · Everyone must use same security algorithm · Ex: AES, DES

→ Ethical Hacking

If using security through obscurity, the first breakins will be from non ethical actors

Creating custom code language is not considered a 'solution' to secure communication

Historical Ciphers:

① Caesar Cipher: Plaintext $\in \{a, \dots z\}^n$

Encoding: $+n \pmod{26}$ $\quad n \in \mathbb{Z}$

Ex: crypto $\xrightarrow{+3}$ FUBSWR

Does not adhere to Kirchhoffs principle

② Shift Cipher: Encoding: $+n \pmod{26}$

$k \in \mathbb{Z}$, k is the key.

Easily brute forced since key space is small though it satisfies Kirchhoffs principle. Does not satisfy principle of large key space

③ Monoalphabetic Substitution Cipher

Shift each letter by a different amount

Key: Permutation of $[0, 1, \dots 25]$ / $[a, b \dots z]$

analogously, $a \to c$, $b \to z$, $c \to d$ ...

Satisfies Kirchhoffs principle & principle of large key space.

Crack: Define p_i as probability of i^{th} character in plaintext, q_i as probability of occurence of i^{th} character in ciphertext.

$\forall i, \exists j \ni p_i = q_j$

Compute q_is

Compute p_is

Match frequencies of p_is with q_js

④ Vigenère Cipher:

Use word as key. Ex: cat

Word: c r y p t o

Key: +2 +0 +19 +0 +19 +

e r . r t .

Crack: Suppose length ℓ is known.

Then Vigenère Cipher is a collection of ℓ shift ciphers

Divide cipher text into multiple shift ciphers of period ℓ: $0, \ell, 2\ell, 3\ell \ldots$

then $\exists k \ni p_i = q_i + k$

Guessing ℓ:

Correct guess: $\sum_{i=0}^{25} p_i^2 \approx \sum_{i=0}^{25} q_i^2$

Wrong guess: $\sum q_i^2 \approx 1/26$