

Theorem: Secure Communication is impossible. Proof: Shannon's Theory  
(Impossibility proofs are different from & harder than possibility proofs)

Definition of security needs to be known to prove impossibility.

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

(Fallability of security through obscurity)

Kirchhoff's argument: Not revealing  $f$  will never be found out  
 $\rightarrow$  can be reverse engineered by human or machine

$\rightarrow f$  is a part of the password (key)

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

$\rightarrow$  Need different algorithms for communication with each actor - does not scale  
 $\rightarrow$  Redesigning virus is hard - like reset password

Why Kirchhoff's Principle is mandatory:

$\rightarrow$  Standardization

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

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

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

Does not adhere to Kirchhoff's principle

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

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

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

③ Monoalphabetic Substitution Cipher

Shift each letter by a different amount

Key: Permutation of  $\{a, b, \dots, z\}$  /  $\{A, B, \dots, Z\}$   
analogously,  $a \rightarrow c, b \rightarrow z, c \rightarrow \dots$

Satisfies Kirchhoff's principle & principle of large key space.

Attack: Define  $p_i$  as probability of  $i^{th}$  character in plaintext,  $q_j$  as probability of occurrence of  $j^{th}$  character in ciphertext

$$\forall i, j \quad p_i = q_j$$

Compute  $q_{j|i}$

Compute  $p_i$ 's

Match frequencies of  $p_i$ 's with  $q_{j|i}$ 's

#### ④ Vigenère Cipher :

Use word as key . Ex : cat

word : c a t p o

Key : c a + t a +  
e t . g 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,  $l$ ,  $2l$ ,  $3l$  ...

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

Guessing  $l$ :

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

Wrong guess:  $\sum q_i^2 \approx 16$