

- J. KATZ + Y. LINDELL

- J. KATZ + Y. LINDELL

POIS

FANTASTIC Q When is a problem Intosac one? **Ans** When the problem is impossible to solve, logically/perfectly.

Will be shown with standard examples.

eg1: hashing password.

theoretically impossible to be perfect if length is not infinite.

eg2: secure communication

@t₀ info(R) = n₀(lev)

A simple circuit diagram showing a battery labeled E_{mf} connected in series with a resistor labeled R . The battery is represented by a long vertical line on the left and a shorter, thicker vertical line on the right. The resistor is represented by a zigzag line. The circuit is a single loop.

② $t > t_0$ info-rec(r) = info-rec(evr)

eg3: Data integrity

If m was sent, modified to m'

and if $m' = 2$ " "

→ It is the same to receiver.

↳ cannot thus identify.



 Eg of non infsec \rightarrow infsec

- problem in distributed computing \therefore now an infsec problem

Solution: use signatures \Rightarrow implying signatures are impossible

FASCINATING Q. How to logically solve/circumvent a logical impossibility?

[Ans] Bring in another impossibility and make it destructively interfere with the original one.

We focus on 4-5 sources of impossibilities in the semester.

Course: See impossibilities

Introduce others

Save them

1 per month Approx

FUNDAMENTAL

Random Words

- Hamming Distance

- information security is God
- all non trivial works of science must include info sec

- logical nego

Sources of Impossibility

① Computational Hardness [Resource Complexity]

Only binary
codes are secure

② Practical Uncertainties

Speed of Light
Quantum Stuff

③ Natural Limits

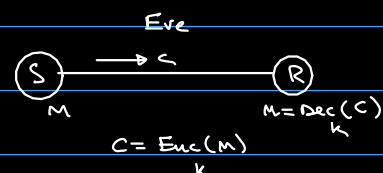
④ Logical / Philosophical Impossibilities

Topics to cover

- Kerckhoffs's Principle
- Designing/ Breaking classical ciphers.

Starting off with secure communication networks.

- traditional ciphers, and how to break them.
- Shannon next class.
 - defined information
 - pathbreaking.

Caesar Cipher

$$C = (x + 3) \% n_c$$

M = message
 C = coded message

n_c = no. of characters in alphabet.

Big talk about his perspective of infosec as an 'art', and a bigger rant on what is art and what is science.

Exact words in book.

Kerckhoffs's Principle

Security of a system must NOT depend on the OBSCURITY of the algorithm, rather must solely depend on the SECRECY of the KEY.

Kerckhoffs's Reasonings

1. Algorithms are reverse engineerable.

eg: $h(x) = bx + c$

Attacker can feed x_1, x_2, \dots, x_n and see that ^{for} all outputs $h(x_1) \dots$

$g \mid h(x_i) - h(x_j)$. And then solve for c .

2. Updation/ Recovery Complexity.

if password random in secure system: change pass.
 if algo " in obscurity " : // fucked.

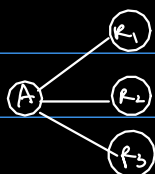
3. Secure Memory is costly.

Proof in modern times: UTM is algo and full input is key.

— bad information storage efficiency.

ASK ATHREYA

4. Scalable



Without: Diff algorithm for everyone.

With: only key changes among people.

Additional Reasoning

1. Ethical Hacking

hypothesis: no system is secure.

bug(algo) will be found because

→ bug exists

→ non ethical people exist

→ only " " search for bug

→ " " will find " "

→ big F, take that L

2. Standards

- needed for efficiency.

- if an algo is used by every system, it should obviously follow

Thus we can see why Caesar cipher fails.

Next iteration:

Shift Cipher:

$$C = (x + k) \bmod n_k$$

M = message

C = coded message

k = key

n_k = no. of characters in alphabet.

→ If key space is small, ^{brute force} attack ez.

first principle learnt:

Principle of large key space

ATTACK

1. Can be broken by humans

2. Autocorrelation:

- frequency analysis

$$p_i = P(\text{ith char in m})$$

$$q_i = P(\text{" " " " c})$$

Precompute $\sum_{i=0}^{25} p_i^2 \approx 0.065$

Now compute $\sum_{i=0}^{25} (p_i q_{i+k})$

$\frac{\text{wrong guess}}{\text{correct guess}} \quad \frac{1/26}{\approx 0.065}$

Next iteration:

Monoalphabetic Substitution Cipher

- Diff alphabets shift by different amts.

- no repetitions allowed

- basically, permutation

for brute force: 26! keys to search \leftarrow applying first principle

Attack

$$\forall i \exists j : q_j \approx p_i$$

\Rightarrow 1. Sort q_i 's } since distribution is same,
2. Sort p_i 's } eg: $p_a = q_n, p_c = q_t, p_t = q_b$

Issue: susceptible to frequency attacks.

Next iteration

Vignere Cipher

1. does not maintain frequency

eg:
$$\begin{array}{r} \text{hello} \\ \text{sease} \\ \hline \text{zlcde} \end{array}$$

FAILED ATTACKS

- brute force: too many keys
- freq anal: freq. not maintained

Can be broken if:

1. key length known
2. " " is findable.

ATTACK

PART 1:

if we know length of key,

partition cipher text into $((\text{length}))$ parts

then shift cipher attack on all $((\text{length}))$ parts.

eg: 3

$C_0 \ C_3 \ C_6 \ \dots$

$C_1 \ C_4 \ C_7 \ \dots$

$C_2 \ C_5 \ C_8 \ \dots$

PART 2:

Guess an l .

take a string $C_0 C_1 C_2 \dots$

$$\text{check if } \underbrace{\sum_{i=0}^{25} q_i^2 = \sum_{i=0}^{25} p_i^2}_{\text{easy}}$$

Topics for 10/01/2020

- Shannon's Perfect Secrecy

- Vernam Cipher is perfect (one-time pad)

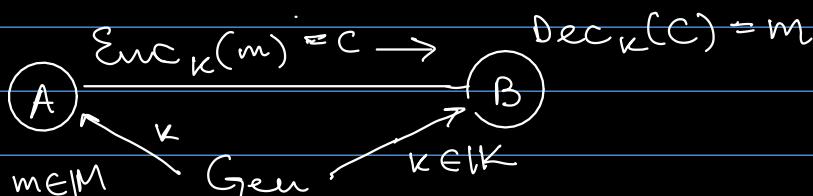
→ Limitations of Shannon's Approach

* Shannon's Perfect Secrecy

Definition of perfectly secure cipher.

An encryption scheme is a 4-tuple

$$\langle \text{Gen}, \text{Enc}, \text{Dec}, \mathcal{M} \rangle$$



$$\text{Dec}_k(\text{Enc}_k(m)) = m$$

Perfectly secret encryption scheme.

An encryption scheme is said to be perfectly secret if for all probability distributions over M , and for all $m \in M$, for all $c \in C$ [where $P(\text{ciphertext} = c) > 0$],

$$P[\text{Message} = m \mid \text{Ciphertext} = c] = P[\text{Message} = m]$$

We will prove one time pad is perfectly secret.

$$P[M=m \mid C=c] = P[M=m]$$

Random Variables.

Vernam Cipher

$$M = K = C = \{0,1\}^n \quad (n\text{-bit space})$$

$$\text{Gen} : K \xleftarrow{R} \{0,1\}^n$$

$$\text{Enc} : C = m \oplus k$$

$$\text{Dec} : m = c \oplus k.$$

- correctness is fairly obvious and not shown here.

$$\begin{aligned} a \oplus a &= 0 \\ m \oplus a \oplus a &= m \oplus 0 = m \\ \text{Dec}_k(\text{Enc}_k(m)) &= m \oplus k \oplus k = m \quad (\text{proved}) \end{aligned}$$

PROOF

First Showing that definition of perfect security is equivalent to

\forall dist over M

$$\forall m \in M, \forall c \in C$$

$$P[C=c \mid M=m] = P[C=c]$$

have to do an iff.

Suppose this holds.

$$P[C=c \mid M=m] = P[C=c]$$

multiply both sides.

$$\left\{ \frac{P[M=m] P[C=c \mid M=m]}{P[C=c]} \right\} = P[M=m]$$

$$\Rightarrow P[M=m \mid C=c] = P[M=m]$$

$$\text{Workability} \propto \frac{1}{\text{Intuitiveness}}$$

Second

showing $\forall c \in C, \forall m_0, m_1 \in M^2$ is eq to 1

$$P[C=c \mid M=m_1] = P[C=c \mid M=m_0]$$

2 \rightarrow 1 is trivial ($P(C=c \mid M=m) = P(C=c)$, $M=m_0$)

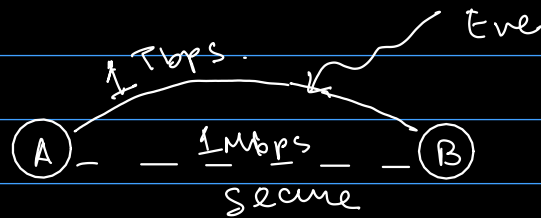
$$P[C=c] = \sum_{m \in M} P[C=c \mid M=m] P[M=m]$$

$$= P \sum_{m \in M} P[M=m] = P$$

The above probability tells us that the encryption of m_0 and m_1 are indistinguishable.

For Vernam Cipher:

$$\begin{aligned} \text{LHS} &= P[C = c | M = m_0] \\ &= P[C = m_0 \oplus k] = P[k = C \oplus m_0] \\ &= 1/2^n = \text{RHS} \quad (P \text{ is not dependent on } m_0) \end{aligned}$$



Uses of Vernam Cipher:

- i) To save your shady business from the feds, encrypt the data and decrypt after raid.
- ii) Use secure channel on low load days to transfer keys and on high load days, use insecure channel by encrypting.

Now, bifurcation in the field.

Symmetric Key cryptography.

Impossible if perfect security.

Two impossibilities

Slow secure channel + fast insecure channel } Fast secure channel

Public Key cryptography

Only insecure channel \Rightarrow slow secure channel

Both are complementary.

Now showing that limitations of Vernam cipher apply to any perfect cipher system as per Shannon's definition.

Minor version of Shannon theorem.

Thm: For any perfectly secret encryption scheme $|K| \geq |M|$

Missing here:

M is compressible.

\Rightarrow no. of bits required to store message is lower bound to no. of bits required to store key.

Shannon did:

$$H(|K|) \geq H(|M|)$$

We use a hacky bypass to this.

ASK ATHREYA FOR INTUITION.

Proof :

Suppose not.

$$|K| < |M|$$

some ciphertext c

$$D = \{m \mid \exists k \in K \text{ Dec}_k(c) = m\}$$

$$\text{now, } |D| \leq |K| \therefore < |M|$$

$$\Rightarrow \exists m^* \in M \text{ s.t. } m^* \notin D$$

consider a dist where $P(M=m^*) \neq 0$

$$\therefore P[M=m^* \mid C=c] = 0$$

but we said $P(M=m^*) \neq 0$

\Rightarrow Scheme is not perfectly secret

\Rightarrow For perfectly secret scheme, $|K|$ must be at least $|M|$.

\therefore one time pad not a one-off.

(the converse)

we will show this directly

implies this cannot be perfectly secret.