Modern Cryptography

Indistinguishability Notion in the Private Key Encryption

Shashank Singh

Perfect Secrecy

Limitation of Perfect Secrecy

- The key space that is at least as large as the message space.

Shannon's Theorem

Let (GEN, ENC, DEC) be an encryption scheme with message space $\mathscr{M}$ for which $|\mathscr{M}| = |\mathscr{K}| = |\mathscr{C}|$, the scheme is perfectly secret if and only if

- Every key $k \in \mathscr{K}$ is chosen with equal probability by the algorithm GEN i.e., $\text{Prob}[K = k] = \frac{1}{|\mathscr{K}|}$.
- For every $m \in \mathscr{M}$ and every $c \in \mathscr{C}$, there exists a unique key $k \in \mathscr{K}$ such that $\text{ENC}_k(m)$ outputs c.

♡

Impracticality of Perfect Secrecy

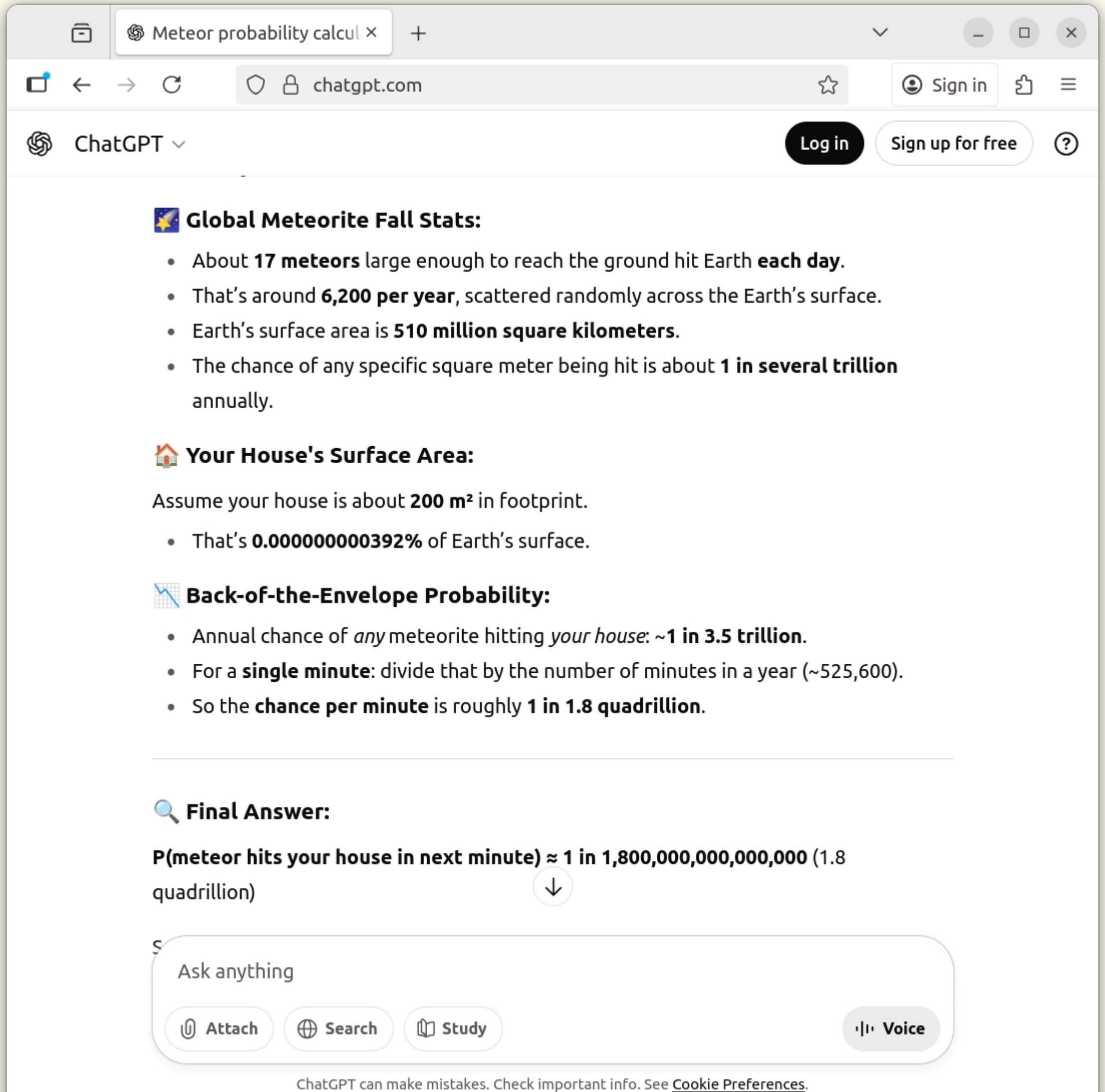
The assumptions behind perfect secrecy are very strict and largely impractical.

- First, the key space must be as large as the message space, which creates significant challenges related to storage and distribution.
- Second, perfect secrecy ensures security against all powerful adversaries. However, in practice, we usually only confront polynomial-time adversaries.
- In the definition of perfect indistinguishability, the experiment must succeed with a probability exactly equal to $\frac{1}{2}$. However, permitting a small, negligible probability advantage for the adversary does not significantly affect the outcome.

- By allowing this minor relaxation, we will later see that we can develop encryption schemes that utilise much smaller keys than those required in perfectly secret schemes.

> **⚠ Warning**
>
> Are we sacrificing too much by allowing such a relaxation?
> - This probability relaxation in the crypto setting is often in the order of $\frac{1}{2^{128}}$.

Probability of a meteor falling on your house in the very next minute



- Thus, we have estimated the probability of a meteor falling on this classroom in the very next minute, which is roughly equal to $\frac{1}{2^{50}}$.
- All of you are still comfortably seated in your chairs without running around.
- Therefore, we can safely allow a negligible probability relaxation for the adversary without practically compromising the security of the scheme.

Private Key Encryption Scheme- Updated Definition

It is defined by three PPT algorithms $\Pi := (\text{GEN}, \text{ENC}, \text{DEC})$ in the security parameter n.

- $k \leftarrow \text{GEN}(n)$. WLOG, we can assume $|k| > n$.
- $c \leftarrow \text{ENC}(k, m)$, for $m \in \{0, 1\}^{\star}$.
- $\perp$ or $m := \text{DEC}(k, c)$

For every n, for every $k \leftarrow \text{GEN}(n)$ and for every $m \in \{0, 1\}^{\star}$, $m = \text{DEC}(k, \text{ENC}(k, m))$.

Computational Indistinguishability for eavesdropper

We define an experiement $\mathrm{PrivK}^{\mathrm{eav}}_{\mathscr{A},\Pi}(n)$ for an encryption scheme $\Pi = (\mathrm{GEN}, \mathrm{ENC}, \mathrm{DEC})$ with parameter n and an adversary $\mathscr{A}$ as follows:

$\mathrm{PrivK}^{\mathrm{eav}}_{\mathscr{A},\Pi}(n)$:

1. $\mathscr{A}$ is given $\Pi(n)$ and it outputs $m_0, m_1 \in \{0,1\}^\star$ with $|m_0| = |m_1|$.
2. $k \leftarrow \mathrm{GEN}(n)$, $b \xleftarrow{\$} \{0,1\}$ and $c \leftarrow \mathrm{ENC}(k, m_b)$ is given to the $\mathscr{A}$.
3. $\mathscr{A}$ return a bit b'.
4. The output of the experiment is $b' \stackrel{?}{=} b$.

♣

Definition 1

A private key encryption scheme $\Pi(n)$ has an indistinguishable encryption in the presence of an eavesdropper, or is EAV-secure, if for all PPT adversaries $\mathscr{A}$, there is a negligible function negl() such that, for all n,

$$\text{Prob}\left[\text{PrivK}^{\text{eav}}_{\mathscr{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \text{negl}(n). \tag{1}$$

♣