

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

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

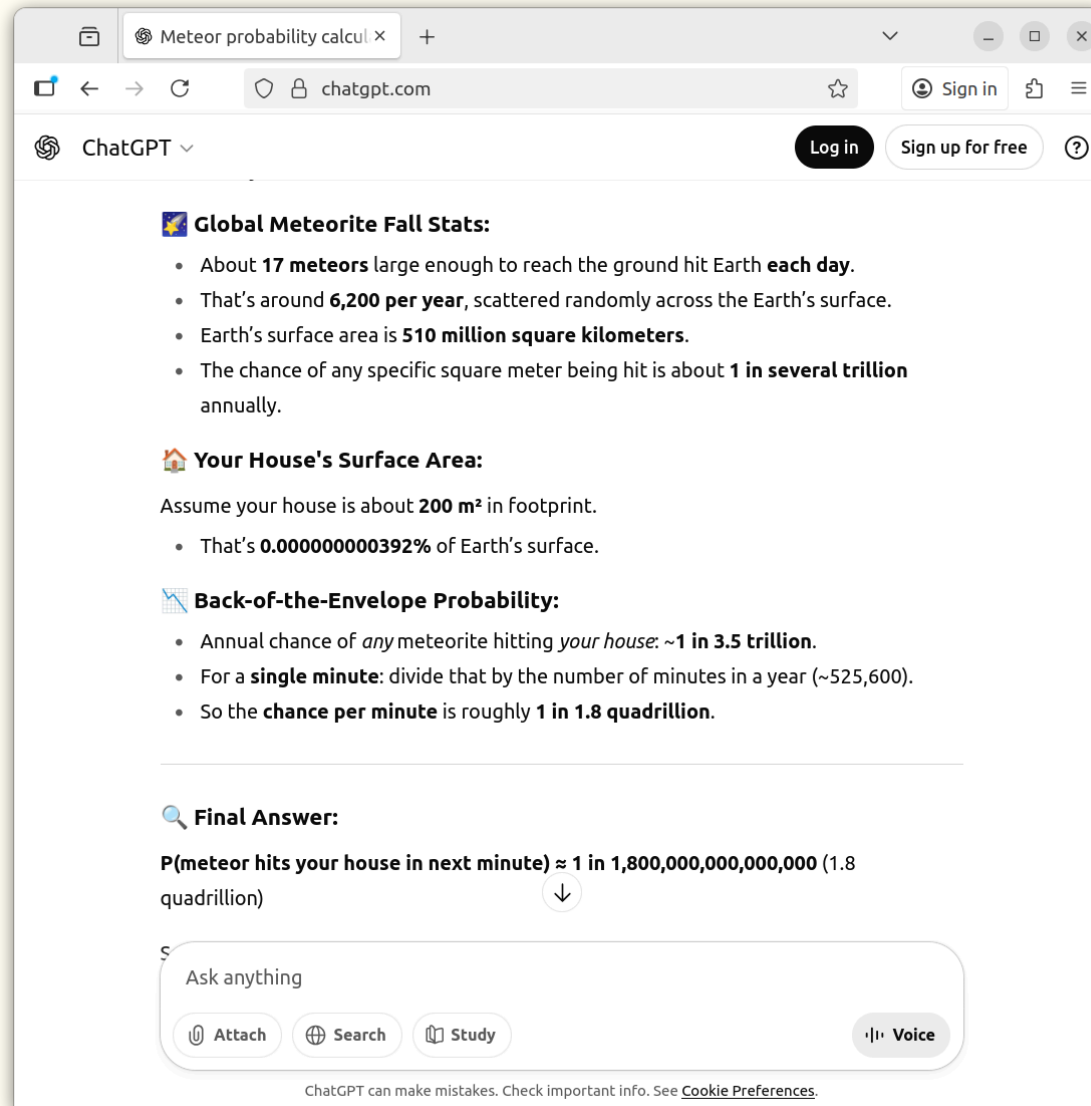
- ▶ By allowing this minor relaxation, we will later see that we can develop encryption schemes that utilise much smaller keys than those required in perfectly secret schemes.

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



The screenshot shows a web browser window with the address bar displaying 'chatgpt.com'. The ChatGPT interface includes a header with the logo, 'ChatGPT', and buttons for 'Log in' and 'Sign up for free'. The main content area is titled 'Global Meteorite Fall Stats:' and lists four bullet points: 'About 17 meteors large enough to reach the ground hit Earth each day.', 'That's around 6,200 per year, scattered randomly across the Earth's surface.', 'Earth's surface area is 510 million square kilometers.', and 'The chance of any specific square meter being hit is about 1 in several trillion annually.' Below this is a section titled 'Your House's Surface Area:' with the text 'Assume your house is about 200 m² in footprint.' and a bullet point: 'That's 0.00000000392% of Earth's surface.' The next section is 'Back-of-the-Envelope Probability:' with three bullet points: 'Annual chance of any meteorite hitting your house: ~1 in 3.5 trillion.', 'For a single minute: divide that by the number of minutes in a year (~525,600).', and 'So the chance per minute is roughly 1 in 1.8 quadrillion.' The 'Final Answer:' section states: 'P(meteor hits your house in next minute) ≈ 1 in 1,800,000,000,000 (1.8 quadrillion)'. At the bottom, there is a search bar with the placeholder text 'Ask anything' and buttons for 'Attach', 'Search', 'Study', and 'Voice'. A footer note says 'ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#)'.

Global Meteorite Fall Stats:

- About **17 meteors** large enough to reach the ground hit Earth **each day**.
- That's around **6,200 per year**, scattered randomly across the Earth's surface.
- Earth's surface area is **510 million square kilometers**.
- The chance of any specific square meter being hit is about **1 in several trillion** annually.

Your House's Surface Area:

Assume your house is about **200 m²** in footprint.

- That's **0.00000000392%** of Earth's surface.

Back-of-the-Envelope Probability:

- Annual chance of *any* meteorite hitting *your house*: **~1 in 3.5 trillion**.
- For a **single minute**: divide that by the number of minutes in a year (~525,600).
- So the **chance per minute** is roughly **1 in 1.8 quadrillion**.

Final Answer:

P(meteor hits your house in next minute) ≈ 1 in 1,800,000,000,000 (1.8 quadrillion)

Ask anything

Attach Search Study Voice

ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#).

- 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 $m \in \{0, 1\}^*$.
- \perp or $m := \text{DEC}(k, c)$

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

Computational Indistinguishability for eavesdropper

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

$\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) :$

1. \mathcal{A} is given $\Pi(n)$ and it outputs $m_0, m_1 \in \{0, 1\}^*$ with $|m_0| = |m_1|$.
2. $k \leftarrow \text{GEN}(n)$, $b \overset{\$}{\leftarrow} \{0, 1\}$ and $c \leftarrow \text{ENC}(k, m_b)$ is given to the \mathcal{A} .
3. \mathcal{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 \mathcal{A} , there is a negligible function $\text{negl}()$ such that, for all n ,

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

