

Chance or Pattern? Learning Cybersecurity through Benford's Law and AI

Raúl Aparicio-Téllez, Gabriel López-Pinar, Roque Fernández, Miguel Garcia-Bosque, Carlos Sanchez-Azqueta, Santiago Celma, Concepción Aldea

Group of Didactics of Electronics with ICT Resources (DIELTIC), University of Zaragoza, Spain

How to cite: Aparicio-Téllez, R.; López-Pinar, G.; Fernández, R.; Garcia-Bosque, M.; Sanchez-Azqueta, C.; Celma, S.; Aldea, C. (2026). Chance or Pattern? Learning Cybersecurity through Benford's Law and AI. In: 12th International Conference on Higher Education Advances (HEAd'26). Valencia, 15-18 June 2026. <https://doi.org/10.4995/HEAd26.2026.21758>

Abstract

This paper presents an innovative learning sequence designed for science and engineering students, specifically within the Master's Degree in Physics and Physical Technologies. The proposal addresses the persistent misconceptions regarding randomness and statistical inference by integrating Benford's Law, Artificial Intelligence (AI), and cybersecurity. Through a Challenge-Based Learning (CBL) methodology, students transition from intuitive, qualitative assessments of data authenticity to quantitative analysis using Python and AI-generated datasets. The sequence leverages “cognitive conflict” to dismantle representativeness bias, fostering critical thinking and ethical reasoning in scientific data handling.

Keywords: *artificial intelligence, Benford's Law, challenge-based learning, cybersecurity, higher education, fraud detection, statistics.*

1. Introduction

The teaching of probability and statistics in science and engineering degrees frequently faces the persistence of misconceptions regarding the nature of randomness. Even in higher education (Sotos et al., 2007; Fiedler et al., 2017), students often carry a deficient understanding of statistical inference, frequently limiting themselves to a mechanical application of formulas without a deep comprehension of data distribution (Bar-Hillel and Wagenaar, 1991). This difficulty is exacerbated by the representativeness bias, whereby students tend to evaluate the probability of a sample based on how similar it is to what they consider “typical” or “random”, ignoring fundamental statistical laws (Hirsch and O'Donnell, 2001).

In the field of modern electronics and Internet of Things (IoT) (Milano and Gómez-Expósito, 2021), these flawed intuitions represent a critical risk, as they prevent future professionals from correctly identifying non-uniform patterns or manipulations in complex datasets. Since current

security depends on the integrity of physical signals and resource constraints in hardware prevent the use of heavy solutions, it becomes essential to employ lightweight statistical analysis methods that allow for the distinction between natural failures and cyberattacks directly at their source.

A particularly relevant example for addressing these contents is Benford's Law, stated by Frank Benford and also known as the First-Digit Law. This law establishes that, in many large sets of numerical data obtained from real-world phenomena, the probability of a number starting with a specific digit is not uniform: the digit 1 appears most frequently as the first digit, and this probability progressively decreases as the starting digit increases toward 9.

Benford's Law has practical applications in various fields, including cybersecurity. In particular, it is used as a tool for detecting fraud and cybercrime. The amounts of legitimate financial transactions typically conform to a distribution close to Benford's, whereas values generated artificially or randomly by fraudsters tend to deviate from it. The analysis of these deviations allows the identification of suspicious patterns and constitutes a powerful didactic example for connecting concepts of randomness, statistics, and computer security within the context of higher education.

2. Methodology

2.1. Context and participants

This proposal is intended for students enrolled in science and engineering programs that include subjects related to randomness or cybersecurity, as well as subjects including contents related to scientific methodologies, ethical issues and fraud detection. The interdisciplinary nature of this work makes it adaptable to different learning environments.

In particular, this work is intended for students enrolled in a Master's Degree in Physics and Physical Technologies at the authors' institution. It has been integrated into a course on scientific methodology, as part of a module dedicated to scientific ethics and fraud detection, with particular emphasis on the role of cybersecurity in detecting and preventing fraudulent practices. The proposed activities encourage reflection on ethical conduct in scientific research, the recognition of fraudulent behaviors, and the responsible use of data and probabilistic reasoning, emphasizing how cybersecurity tools and principles contribute to data integrity and the detection of manipulation.

2.2. Design of the learning sequence

In this work, a learning sequence centered on the concept of randomness and its implications across different areas of the society is proposed. To this purpose, a sequence of two activities designed under the methodology of challenge-based learning (CBL) is implemented (Figure 1).

The first activity is qualitative. Its aim is for students to reflect on the concept of randomness and its importance in different areas of society through practical examples, fostering critical thinking and problem identification. The second activity is quantitative, requiring students to design, analyze, and evaluate solutions, integrating the knowledge they have acquired while developing reasoning, collaboration, and decision-making skills.

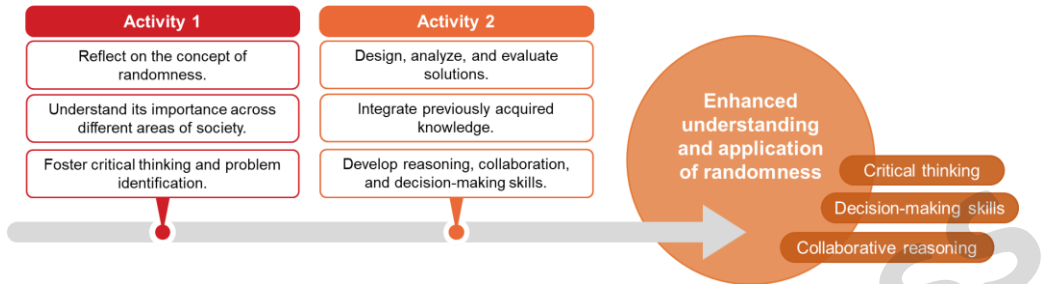


Figure 1. Learning process proposed in the teaching sequence.

Throughout the learning sequence, students are encouraged to reflect on their own learning process, identify strengths and connect theoretical concepts with their practical applications. This way, by addressing real-world problems and ethical challenges, this sequence aims to foster both professional skills and higher-order cognitive abilities, preparing students to apply their knowledge critically and responsibly in various scientific and professional areas.

2.3. Activity 1. “Fraud hunters”: Developing intuition on randomness

In this first activity, students are organized into heterogeneous groups of 3–4 members. Each group receives several short sets of numerical sequences from different sources, without any additional information about their origin.

The main task for each group is to classify the sequences by visual inspection, without performing calculations or using analytical tools. Each group must decide whether the data appear natural or artificial, justifying their decision based on intuitive criteria. Most students find this classification very challenging, as their intuitions about what constitutes “random” or “normal” are often unreliable and do not match the actual patterns in the data.

For example, one of the real sequences consists of the first digits of the population numbers of Spanish cities according to Wikipedia. Although both sequences appear equally “irregular” at first glance, people are generally unable to classify them correctly, highlighting the difficulty of judging data authenticity without formal statistical analysis. This type of example helps illustrate how human intuition can fail and sets the stage for introducing Benford’s Law as a tool for detecting patterns and anomalies.

The activity concludes with the visualization of a video explaining that these patterns are not the result of chance, and that they reflect a phenomenon already studied and known as Benford's Law. This activity deliberately introduces a cognitive conflict by confronting the intuition of students about randomness, which is often associated with uniformity or the absence of patterns, with empirical evidence.

The classification errors that emerge reveal the limitations of intuitive reasoning and create the need for more formal analytical approaches, which are addressed in the next activity.

2.4. Activity 2. "Hackathon": Data generation and analysis using AI

In the previous activity, students are expected to have already been able to identify intuitive patterns in numerical sequences and recognize the limitations of their reasoning at first glance. Therefore, at this stage of the learning sequence, students start from the understanding that the appearance of randomness does not always reflect the actual nature of the data. The second activity is focused on quantitative analysis.

In the first part, each group of students is asked to search online for a certain number of real datasets that follow Benford's Law and to generate an equal number of artificial datasets that do not follow this distribution using ChatGPT. The use of AI is particularly valuable in this activity, as it allows students to quickly create synthetic data simulating different patterns without relying on confidential information, while also working with publicly accessible real data. This approach facilitates experimentation and fosters understanding of how statistical patterns emerge or are altered in different contexts.

The second part of the activity is organized as a hackathon. All the datasets (both real and synthetic) created by the groups are combined, and each group is asked to analyze the sequences using statistical and programming tools such as Python. For each dataset, students extract the first digits, calculate their frequencies, and compare the observed distribution with Benford's Law, evaluating significant deviations and potential anomalies. Finally, students must interpret the results of the hypothesis tests to determine whether the data are genuine or fabricated. This learning process is summarized in Figure 2.

At the end of the hackathon, the results are presented and a group reflection is conducted on the effectiveness of Benford's Law for detecting anomalies, as well as its limitations as a sole analytical tool.

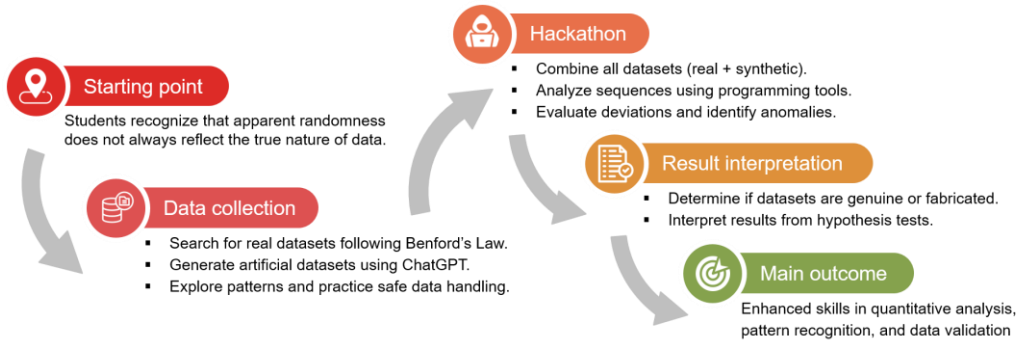


Figure 2. Design of the learning sequence of the second activity.

3. Implementation and assessment

The implementation of this learning sequence follows a continuous and formative assessment model, ensuring that the evaluation is not merely a final grade but a fundamental part of the learning process itself.

3.1. Assessment strategy

The evaluation is structured around three key pillars:

- **Process-oriented feedback:** During the "Fraud hunters" activity, the assessment focuses on the quality of the arguments used to justify the initial classification. The "error" (misidentifying a sequence) is used as a pedagogical tool to trigger cognitive conflict, rather than a point deduction.
- **Technical proficiency:** In the "Hackathon" phase, the ability of students to manipulate data using Python and interpret statistical deviations from the Benford distribution is evaluated.
- **Reflective practice:** Students must submit a final report where they reflect on how their understanding of randomness evolved from Activity 1 to Activity 2.

3.2. Impact on student learning

The integration of this learning sequence provides several pedagogical benefits that enhance the students' academic and professional profile. First, the use of real-world cybersecurity scenarios and AI tools like ChatGPT shifts the perception of statistics from a purely theoretical requirement to a practical, "detective-like" skill. By framing the analysis as a fraud-detection challenge, student engagement increases significantly as they perceive the immediate utility of the mathematical tools.

Furthermore, the sequence facilitates the deconstruction of cognitive biases through a structured cognitive conflict. By systematically failing the initial intuitive test in Activity 1, students recognize the limitations of their own judgment, making them more receptive to formal analytical methods. This transition is essential for effectively dismantling the representativeness bias and understanding the counter-intuitive nature of the Benford's Law.

Beyond the technical aspects of physics and mathematics, the activity also fosters the development of transversal and ethical skills. It promotes an ethical awareness regarding data integrity and scientific fraud, preparing students for professional environments where data manipulation represents a constant threat. This approach emphasizes the social responsibility of the scientist and the importance of cybersecurity in maintaining the reliability of empirical evidence.

Finally, the sequence contributes to the enhancement of AI literacy. Using generative AI to create synthetic datasets allows students to explore the underlying patterns of Large Language Models (LLMs) and their current limitations in mimicking natural distributions. This interaction provides a critical perspective on the use and reliability of AI in scientific contexts, teaching students to identify the subtle differences between data derived from natural phenomena and that generated by artificial algorithms.

4. Conclusions

The pedagogical proposal presented in this work is designed to demonstrate that the integration of Benford's Law and AI can provide a robust framework for teaching probability and statistics in higher education. By confronting students with the limitations of their own intuition regarding randomness, the proposed learning sequence aims to bridge the gap between theoretical knowledge and practical application in cybersecurity. This approach is structured on the premise that cognitive conflict, when applied through challenge-based learning, serves as an effective catalyst for overcoming deeply rooted statistical biases, such as the representativeness heuristic.

Furthermore, the strategic use of AI tools like ChatGPT as synthetic data generators is intended to offer a dual benefit: facilitating the creation of diverse datasets for analysis while providing a critical space for students to evaluate the current capabilities and limitations of Large Language Models in mimicking natural phenomena. This interaction is expected to be crucial for developing a form of AI literacy, where students learn to treat AI-generated output with the same analytical rigor as any other data source.

In conclusion, the sequence is developed not only to strengthen technical skills in programming and statistical inference but also to reinforce an ethical commitment to data integrity. In an era where IoT devices and physical signals are increasingly vulnerable to manipulation, training

scientists and engineers to identify non-uniform patterns through lightweight statistical methods becomes essential. This work proposes that interdisciplinary methodologies, which connect classical mathematical laws with contemporary technological challenges, can significantly enhance student motivation and better prepare them for the complex professional demands of the modern scientific landscape.

References

- Bar-Hillel, M., & Wagenaar, W. A. (1991). The perception of randomness. *Advances in applied mathematics*, 12(4), 428-454.
- Fiedler, D., Tröbst, S., and Harms, U. (2017). University students' conceptual knowledge of randomness and probability in the contexts of evolution and mathematics. *CBE—Life Sciences Education*, 16(2).
- Hirsch, L. S., and O'Donnell, A. M. (2001). Representativeness in statistical reasoning: Identifying and assessing misconceptions. *Journal of Statistics Education*, 9(2), doi: 10.1080/10691898.2001.11910655.
- Milano, F., and Gómez-Expósito, A. (2021). Detection of Cyber-Attacks of Power Systems Through Benford's Law, in *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2741-2744, doi: 10.1109/TSG.2020.3042897.
- Sotos, A. E. C., Vanhoof, S., Van den Noortgate, W., and Onghena, P. (2007). Students' misconceptions of statistical inference: A review of the empirical evidence from research on statistics education. *Educational research review*, 2(2), 98-113, doi: 10.1016/j.edurev.2007.04.001.