OZ CRYPTO-BATTLE

WHO DECRYPTS FASTER? AI SYSTEMS OR CLASSIC ALGORITHMS?

So, who managed to decrypt the text faster? And what exactly does this task have to do with Artificial Intelligence?

When comparing the methods you and your fellow player used, you can see how „normal“ algorithms, which you may already know from CS class, differ from the approach of AI systems.

How does a classic algorithm work?

An algorithm is always programmed by a human. It is important to precisely specify what the computer should do. So, the human must first analyze exactly what needs to be done and formulate the algorithm‘s instructions precisely. These instructions are then executed step by step by the program. Each step must be precisely defined. If that is not the case, the program code cannot be executed – you‘ve probably experienced this yourself while programming.

To decrypt the text, you or one of you had the task of composing an algorithm that gives precise instructions on how the letters should be shifted to decrypt the text. This shows how important it is to make exact and precise specifications: Whether the letters are shifted, for example, by 10 or 9 positions makes the difference between understandable, decrypted text and gibberish. How exactly a procedure works must be decided by the human and specified as program code. However, this can be quite complicated and time-consuming for complex problems. And sometimes it‘s not even possible if no solution options for a problem are known.

How does a data-based AI system work?
If you've already worked at some other stations in the lab, you may already know that AI systems are capable of learning behavior, patterns and relationships. However, they need data that serves as examples to find out how a behavior works or what patterns exist. In a so-called training process, the system analyzes this data and constructs a corresponding model.

You did the same thing when decrypting the text: You were given some example words that were presented to you as plaintext and as encrypted text. This allowed you to see which letters were mapped to each other by encryption and figure out how far the letters were shifted. This made it possible for you to decrypt letters that did not appear in the example words. So, based on examples, you created some rules for how the encryption works. Without examples, i.e. without corresponding datasets, this would not have been possible for you as an „AI system."

In this way, AI systems can also learn various tasks without developing a precise algorithm and programming it themselves. This is especially practical for complex, difficult-to-understand problems where it is not easy to recognize how a problem can be solved. Here, it is sufficient to give the AI system examples of how to proceed, and it can determine the relationships and patterns therein by comparing all examples precisely.

If this is so practical, why don't we just use AI algorithms everywhere?
The answer is quite simple: Five example words, as in this task, are not enough for an AI system; it needs many thousands of examples to be able to recognize meaningful patterns. Often, there is not so much data available, and it would need to be collected first. However, this is not always so easily possible, as either an adequate amount of data is not available, or, for example, private data of individuals would be needed, which can also be problematic in terms of misuse. And sometimes it is also much easier and faster to write an algorithm than to collect data and train an AI system with it, as collecting and training can take longer for simple problems than programming it oneself.

07 CRYPTO-BATTLE

SOURCES