NAME

seedseeker − PRNG reversal tool

SYNOPSIS

This program has 3 main usage modes

Reversal mode:

e.g.: python −m seedseeker −r

Reads a sequence of integers (one per line) from the input, stopping at EOF or empty line. Then tries to reverse the generator that produced it and it's state. For each generator where the reversal is successful, a line with its name and state will be printed to output.

Generation mode:

python −m seedseeker −g <name> <arguments> [−l <total>]

Generates <total> numbers using the generator <name> with the specified <arguments>. The expected formats for generator arguments are detailed in the full documentation.

Prediction mode:

python −m seedseeker −p [−l <total>]

Reads reversed generator states from the input and predicts the next <total> values. Default <total> is 16 and can be changed with the −l flag.

Generally, the program reads input from stdin and writes output to stdout (and errors to stderr). This behavior can be modified using the −i and −o flags.

EXAMPLE

python −m seedseeker −g mersenne 12345 −l 1000 −o sequence.txt

python −m seedseeker −r −i sequence.txt −o reversed.txt

python −m seedseeker −p −l 10 −i reversed.txt

DESCRIPTION

A tool with the ability to infer internal parameters of PRNGs from a sufficiently sized data sample.

−h, −−help

Show a shortened version of this manual.

−g, −−generate <name> <arguments>

Generates numbers by generator <name> with initial state defined by <arguments>. The number of generated values defaults to 16 and can be changed with the −l flag. This default is intended for human readability, it is recommended to use a larger number of values when trying to reverse or otherwise analyze the sequence.

−l, −−limit <total>

Length of the sequence generated/predicted or limit on the length of the sequence to be reversed. Default is 16 or 1024 respectively.

−r, −−reverse

Tries to reverse the given sequence of numbers from input. Prints generator name and state for every generator where the reversal succeeded. The state should match the end of the input sequence (or the point, where it reaches the limit specified with −l).

Note:

For some generators reversal can be quite dependent on the arguments of the generator.

This tool works best if the generators have "good" initial arguments, in degenerate cases the output may not match the expected results (for example, LCG works best if the multiplier is coprime with the modulus).

−p, −−predict
: Predicts future values from a given generator state(s) in the format returned by −r. The number of generated values defaults to 16 and can be changed with the −l flag.
For example:
python −m seedseeker −r −i values.txt −o gen_state.txt
python −m seedseeker −p −l 10 −i gen_state.txt

−i, −−input <file>
: The program will read input from the specified file.

−o, −−output <file>
: Output of the program will be written to the specified file.

−v, −−version
: Program version

SEE ALSO

dieharder(1)