1)

A)

Smart black box fuzzing – Uses some information about the expected input format. The SUT is executed without being modified.

Dumb grey box fuzzing – Has no information about the input domain but the SUT is instrumented to reveal information such as coverage.

Advantage of first one – Allows high speed fuzzing as no modifications are required.

Advantages of second – Allows us to use the feedback to direct the fuzzer

B)

For:

Fuzzers such as AFL have found bugs in many popular pieces of software including OpenSSL and the iOS kernel. In a security critical library such as OpenSSL all bugs should be fixed so that they can’t lead to an exploit.

Fuzzers are useful not just for security critical bugs. Finding and fixing bugs that come up improves the quality and stability of the application. Especially useful if your software has a lot of users.

Fuzzing explores scenarios that may happen but were an oversight in designing of tests.

Against:

Fuzzing can take a lot of time and manual effort. We saw how fuzzing some program might continuously find the same bug until it is fixed. So this is a process that takes a long time.

Many, if not all of the bugs that are found might be very minor that will be never actually come up in real use. The time/money needed to fix such bugs makes it not worth it.

The inputs generated by fuzzing can be difficult to read, making it difficult for developers to debug and fix errors using provided inputs.

C)

IsCyclic metamorphic transformation: for every node with degree 1, create a copy of it that hooks off the same parent.

ShortestPath metamorphic transformation: ...

D)

To ensure avoidance of undefined behavior, compile the SUT with compiler sanitizers (e.g. UBSan) to detect undefined behavior. Then create a smart, mutation-based grey-box fuzzer that creates well-formed pdf documents and mutate them to create partially erroneous pdfs and observe the outputs. Instrument code with coverage to form feedback to prioritize mutation of inputs that generate new coverage. To ensure pdf appears correctly, crosscheck between established pdf viewers and check that viewpdf outputs the same render.