What is cryptanalysis?

Let’s use symmetric encryption algorithm or the box with the built-in lock as an example. Traditionally, when people start to build the box and the lock, they may encounter a lot of problems which may be escalated into security issues. The box may have some holes that can only be seen through microscope. The box hardness may not be hard enough and need to find possible material to further hardening the box. You start to get the idea.

What cryptanalysis does is to further strengthen the algorithm or box so that they are consider “safe and secure” enough. The most commonly known symmetric encryption algorithm such as AES have gone through a lot of testing which normally involves with computers and mathematics, the numerous testing and rightful alteration ensures that AES is safe and secure enough to use as a modern industry symmetric encryption algorithm. Just like the box, you wouldn’t want a box that has big holes and not hard enough. By going through different testing and alteration, you ended up with an almost indestructible box that has been shown in the symmetric encryption document.