Authentication

Created	@December 10, 2022 11:42 AM
Tags	

Problem:

Ensure message authentication and integrity.

Steps:

Most important step is taking the problem and turning it into primitive simple problems. These have to be well defined because failure in one of these steps results in the failure of the task. So if the task is “ensure the integrity of the file being sent”, the more primitive tasks would be “read the file”, “run it through a MAC algorithm”, “how to attach it to the file” … For these kinds of problems it is useful to draw a diagram of the actions needed to be taken and seeing if they are implemented properly.

Security:

Important to choose a key that is safe, meaning it has high entropy, good algorithms for encryption and hashing and making sure that the code written doesn’t have hard coded keys.