

Figure of the Protocol used in part 3

Program A3 us responsible for Generating a HMAC and sending it to program B3.

Program B3 is responsible for generating HAC and compare A3 HMAC with the one generated, to find evidence of integrity errors an authenticate the file’s sender.

To generate the HMAC, the message and the symmetric key is used. The HMAC protocol uses the key and have 2 passes at hashing the message + signature. This can prevent length extension attacks.

When Program B3 get the message, B3 can generate a HMAC using the same data and check if A3’s HMAC matches B3 HMAC. If true, the message is authenticated, and the integrity is sound.