Informe Inicial PDP

David Castillo Cabello

2017-10-07

Despres d'assolir els coneixements necessaris i recopilar informació sobre l'article "Scalable and efficient Provable data possession", he decidit que tant els algoritmes hash com les funcions MAC estaran basats en SHA-256 i HMAC-SHA256, per altra banda, la implementació tant del servidor com del client seran en Python 3.6 ja que és un llenguatge amb el que estic molt familiaritzat i té les llibreries i tecnologies necessaries per dur a terme totes les tasques d'aquest algorisme.

En quant al disseny de l'aplicació primer em centraré en la fase de setup i, una vegada el client ja faci el xifrat de les dades, treballaré en refinar la comunicació entre el client i el servidor, que actualment ja estan comunicats mitjançant sockets.

Centrant-me en la fase de setup, com abans he dit, els algolitmes MAC i Hash estaran basats en SHA-256 i les claus binaries que utilitzaran les funcions i permutacions random per indexar el resultat seran de longitud variable però fixades per defecte a 128 bits o 256 bits.

La planificació temporal del treball és la següent:
Part del mes de setembre i el mes d'octubre l'he dedicat a fer recerca dels algorismes Hash del que parla el paper, i a començar a planificar el diagrama de clases del projecte. Durant el mes de novembre acabaré d'implementar la fase de Setup i si hi ha cap dubte començaré amb les consultes. Si tot va segons el plan el desembre el podré dedicar a montar la comunicació entre client i servidor, montar un servidor amb un sistema de fitxers i poder pasar-li les dades del client. A més ja començar a treballar en la fase de verificació per tal de poder ampliar el projecte al gener.