NIS Project Writeup

Josh Buchalter, Andreas Von Holy, Alon Bresler, Osher Shuman
BCHJOS003, VHLAND002, BRSALO001, SHMOSH001

Department of Computer Science, University of Cape Town, Rondebosch 7701,
Cape Town, South Africa.

March 29, 2016

Abstract

A writeup detailing the implementation details of our secure client-server system.

1 Introduction

We were tasked with creating a secure client-server communication system that implemented the practices laid out in PGP security. These practices are namely, message confidentiality and authentication. In this writeup, we document the implementation of these practices as well as detailing the choice of language the system is written in, the algorithms used, key management and finally communication connectivity model.

2 Implementation

The process of providing message confidentiality and authentication, as laid out in PGP, is shown below and formed the basis for our implementation.

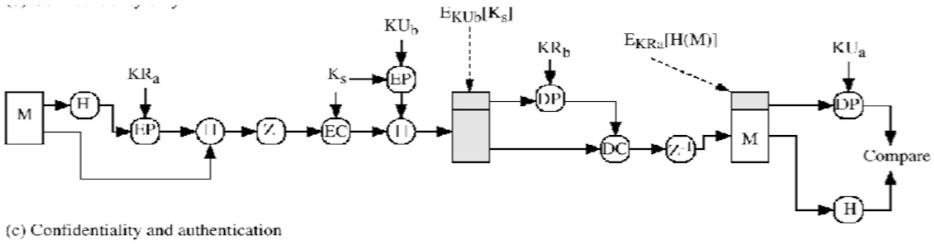

Figure 1: The full PGP process

2.1 Client

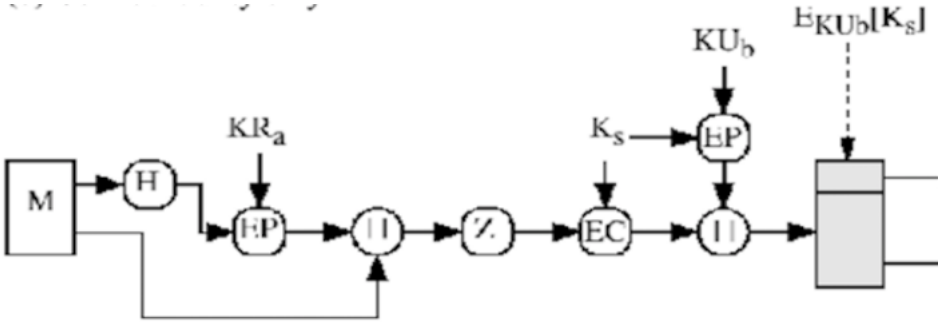

Figure 2: Encryption process done by the client

2.2 Server

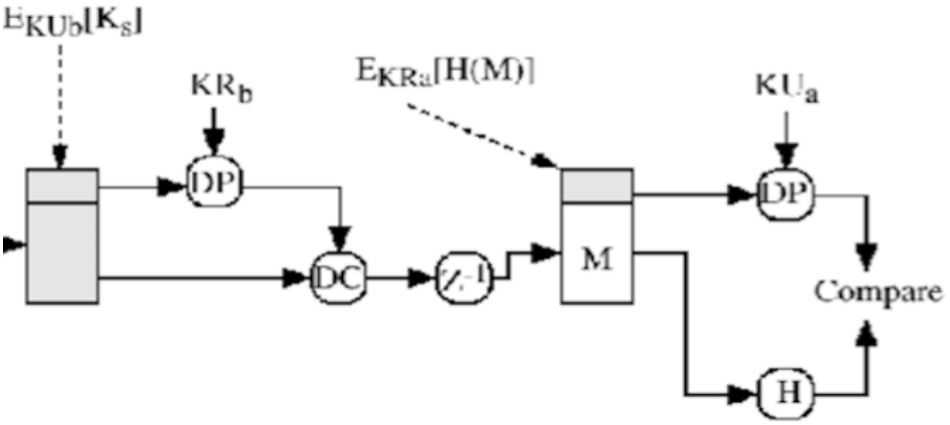

Figure 3: Decryption process done by the server

3 Choice of Language

Choice of Language here..

4 Choice of Cryptographic Algorithms

Choice of crypto algorhtms here..

4.1 Encryption

Encryption algs here..

4.2 Decryption

Decryption here...

5 Key Management

Key Management here...

6 Communication Connectivity Model

Comms connectivity model here...

7 Conclusion

Conclusion here.. (if necessary)