COMP3334 Computer System Security Assignment 2

Poon Yat Sing (13040015D) <star.poon@connect.polyu.hk>

Abstract—**This document provides the compilation procedures, execution instructions, design concerns and implementation details of of the Password-Based Authentication System. We will discuss the assumptions and requirements of the system. We will also compare different existing tools and explain the choice of libraries used in the system.**

Keywords*—*Scrypt, key derivation function, Galois/Counter Mode(GCM), AES, RSA, Digital Signature, password storage, salt, Authenticated Encryption (AE)

I. Compilation

```
Put your code here.
```

References

[1] libscrypt. https://github.com/technion/libscrypt

[2] Assurance Technologies. *Modular Crypt Format*[Online]. Available:
https://pythonhosted.org/passlib/modular_crypt_format.html
http://stackoverflow.com/questions/1220751/how-to-choose-an-aes-encryption-mode-cbc-ecb-ctr-ocb-cfb
http://cseweb.ucsd.edu/ mihir/papers/oem.pdf
http://crypto.stackexchange.com/questions/6842/how-to-choose-between-aes-ccm-and-aes-gcm-for-storage-volume-encryption
http://hayageek.com/rsa-encryption-decryption-openssl-c/
http://web.cs.ucdavis.edu/ rogaway/papers/modes.pdf

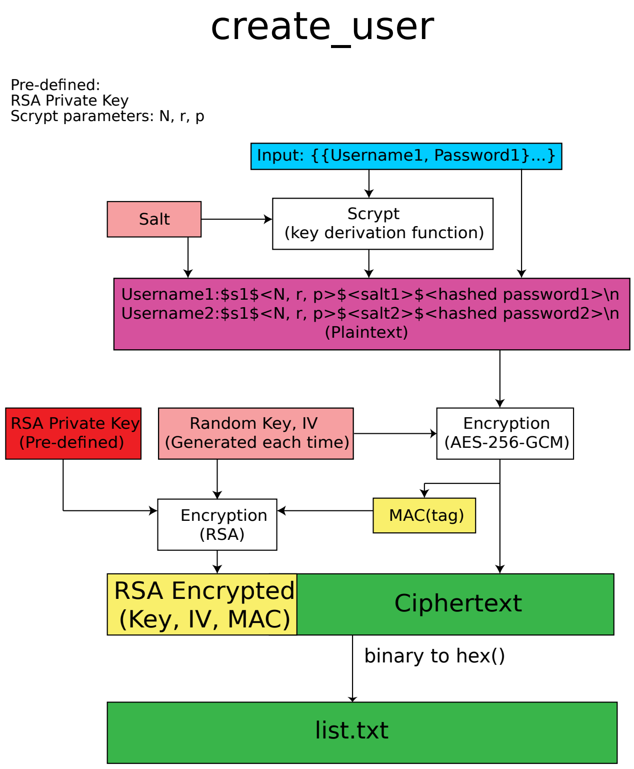

Fig. 1. Workflow of create_user module

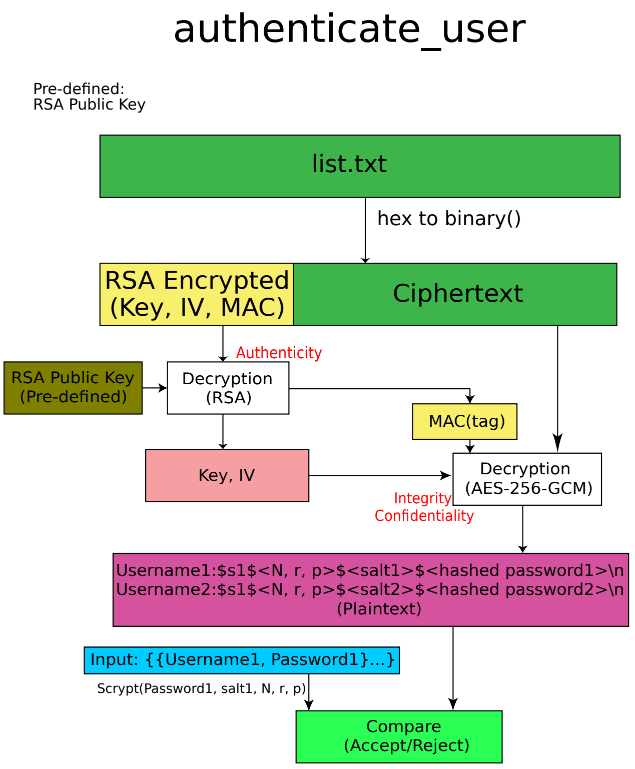

Fig. 2. Workflow of authenticate_user module