Advanced Software Engineering Techniques - Requirements Analysis

Cotan Paul Adrian, Kelesidis Evgnosia Alexandra

January 2020

1 Introduction

1.1 Application's overview

Clifford Cocks proposed in 2001 an *identity-based encryption* or *IBE* scheme. This application generates an encrypted message.

1.2 Constraints

Clifford Cocks proposed a scheme where the encryption is made bit by bit, so the speed is heavily affected by the size of the message and, moreover, the cipher text size is much larger than the size of the message when has been used an 1024 or 2048-bit key (recommended values).

1.3 Actors

- The end user
- The Cocks Algorithm
- The message
- The encrypted message
- The e-mail

1.4 Possible clients

As we said before, Cocks' IBE is used for encrypting files. Usually it is used to encrypt short passwords or session keys for other applications using a personal ID. Considering this facts, any company which needs to communicate short messages to its employees via e-mail or another platform and needs the security of the message will be interested in this application.

2 Use case

2.1 Encryption

1. On opening the application, the and user has to choose whether he want to encrypt or decrypt a message.

2. After choosing the encryption process, the end user will have to write the receiver's ID and the message. If the sender enters a wrong ID or a too long message, the application will send an error.

3. If both ID and message's length are good, the program creates "Messag3.txt" file with the encrypted message.

4. The end user will send the file via e-mail or another platform or way.

2.2 Decryption

1. The end user notice he received an encrypted file from his/ her company via e-mail or another platform or way.

2. On opening the application, the and user has to choose whether he want to encrypt or decrypt a message.

3. After choosing the decryption process, the end user will have to write his/ her own ID and to put the received "Messag3.txt" file in the folder. If the receiver's ID is wrong or the file is not in the folder, the application will send an error.

4. If both conditions are satisfied, the application will output the message.