3. Design

Save the file's!!

Student No.	22110611
Name	문성윤
E-mail	castle9612@gmail.com

[Revision history]

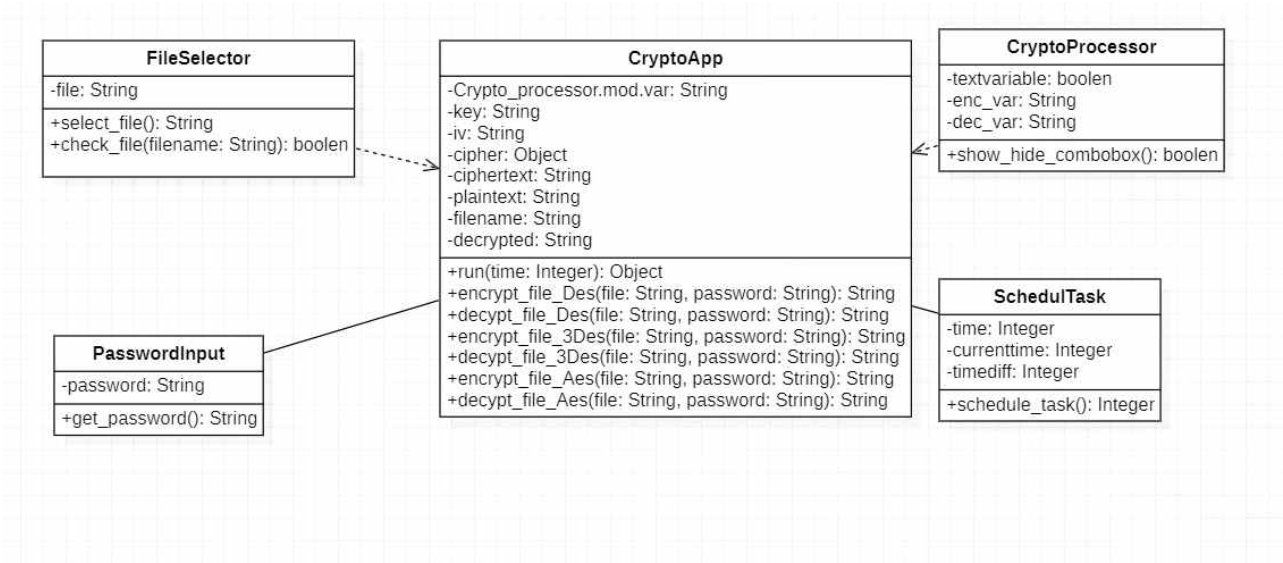
Revision date	Version #	Description	Author
03/30/2023	1.0.0	First Draft	문성윤
05/05/2023	1.0.1	초기버전	문성윤

= Contents =

1. Introduction

- Summarize the contents of this document. - Describe the important points of your design. - 12pt, 160%.

2. Class diagram



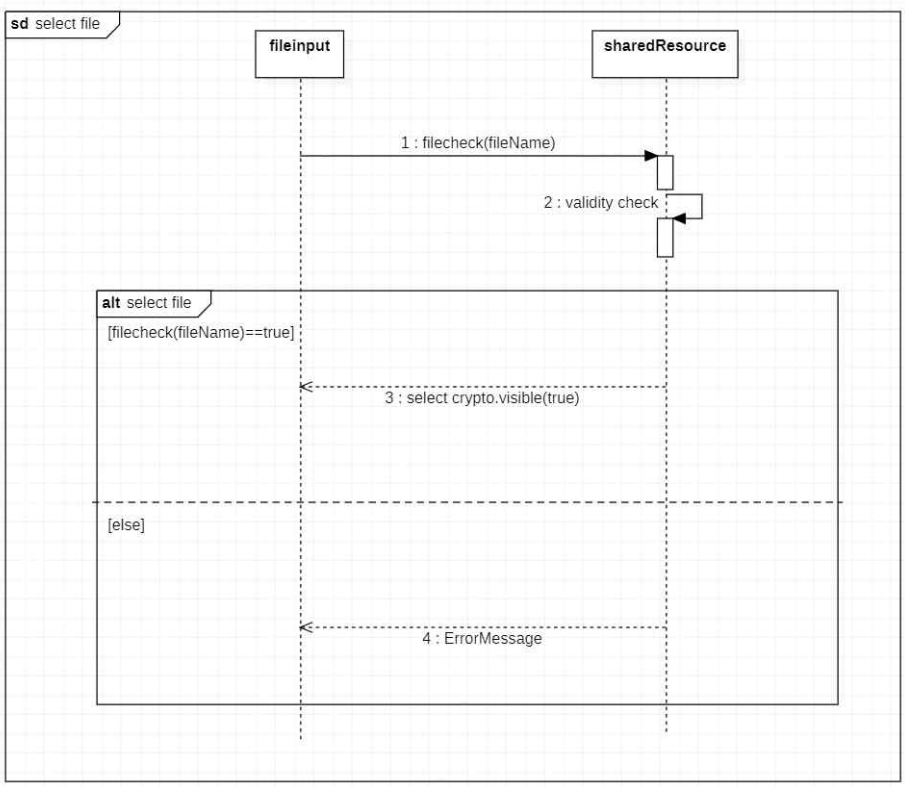
Class Name	Explanation
FileSelector	암호화/복호화 할 파일(들)을 선택하고 파일(들)을 선택했는지 안했는지 검사하는 클래스이다. selector_file():파일을 선택하며 파일의 이름과 내용을 반환하는 함수이다. check check_file(filename:String):파일의 이름을 가져와 파일의 이름이 none이면 파일이 선택되지 않은 것으로 파일을 선택하라는 오류 메시지를 보내거나 파일의 이름이 있다면 true를 반환하는 함수이다.

PasswordInput	파일의 암호화/복호화를 할 때 파일을 암호를 설정해주는 클래스이다. get_password():사용자가 파일의 암호를 입력한대로 가져와 password라는 변수에 저장하는 함수이다. 만약 사용자가 암호를 입력하지 않는다면 시스템에서 제공하는 기본암호를 사용하여 password변수에 저장을한다.
CryptoProcessor	파일의 암호화를 할지 복호화를 할지 정하는 클래스이며 암호화 복호화 선택후 무슨기법으로 암호화/복호화 할것인지 선택하는 클래스이다. show_hide_combobox():파일의 암호화/복호화 선택후 기법선택창을 사용자 화면에 띄우는 함수이며 기법선택창에서 기법을 선택시 암호화/복호화 기법을 반환하는 함수이다.
schedulTask	사용자가 입력한 시간대에 자동으로 암호화/복호화 할수있도록 사용자가 시간을 입력하고 현재시간이랑 비교하여 암호화/복호화가 작동하는 클래스이다. shedule_task():사용자가 시간대를 입력하고 현재시간을 가져와 비교하여 일정시간이후 암호화/복호화가 작동하도록 하며 만약 사용자가 시간을 입력하지 않는다면 그즉시 암호화/복호화가 작동하도록 해주는 함수이다.
CryptoApp	사용자가 선택한 암호화/복호화 기법을 실행하는 클래스이며 사용자가 실행버튼을 누르면 실행이 되도록 하는 클래스이다. run(time:Integer): 사용자가 입력한 시간을 가져와 사용자가 실행을 누르면 사용자가 입력한 시간에 파일의 암호화/복호화가 작동하도록 하는 함수이다. encrytp_file_DES(file:String, password:String): 파일의 내용을 가져와서 DES기법으로 사용자가 입력한 암호를 가져와 파일을 암호화 후 암호화된 내용으로 반환하는 클래스이다. encrytp_file_3-DES(file:String, password:String): 파일의 내용을 가져와서 3-DES기법으로 사용자가 입력한 암호를 가져와 파일을 암호화 후 암호화된 내용으로 반환하는 클래스이다.

	encrytp_file_AES(file:String, password:String): 파일의 내용을 가져와서 AES기법으로 사용자가 입력한 암호를 가져와 파일을 암호화 후 암호화된 내용으로 반환하는 클래스이다. decrytp_file_DES(file:String, password:String): 파일의 내용을 가져와서 DES기법으로 사용자가 입력한 암호를 가져와 파일을 복호화 후 복호화된 내용으로 반환하는 클래스이다. decrytp_file_3-DES(file:String, password:String): 파일의 내용을 가져와서 3-DES기법으로 사용자가 입력한 암호를 가져와 파일을 복호화 후 복호화된 내용으로 반환하는 클래스이다. decrytp_file_AES(file:String, password:String): 파일의 내용을 가져와서 AES기법으로 사용자가 입력한 암호를 가져와 파일을 복호화 후 복호화된 내용으로 반환하는 클래스이다.

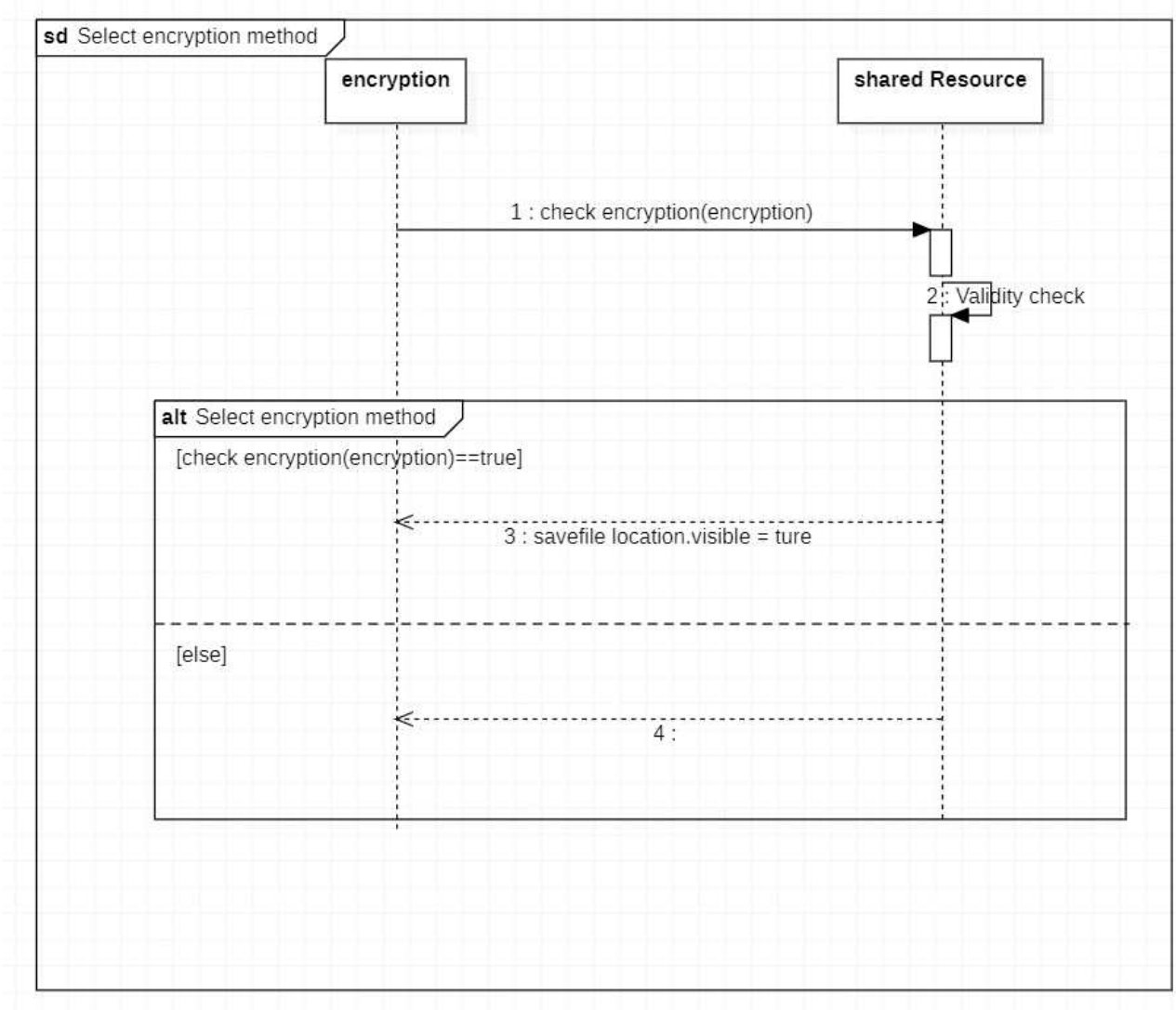
3. Sequence diagram

아래에 나오는 그림들은 Conceptualization에서 표현한 기능들을 Sequence Diagram으로 나타낸 그림들이다.



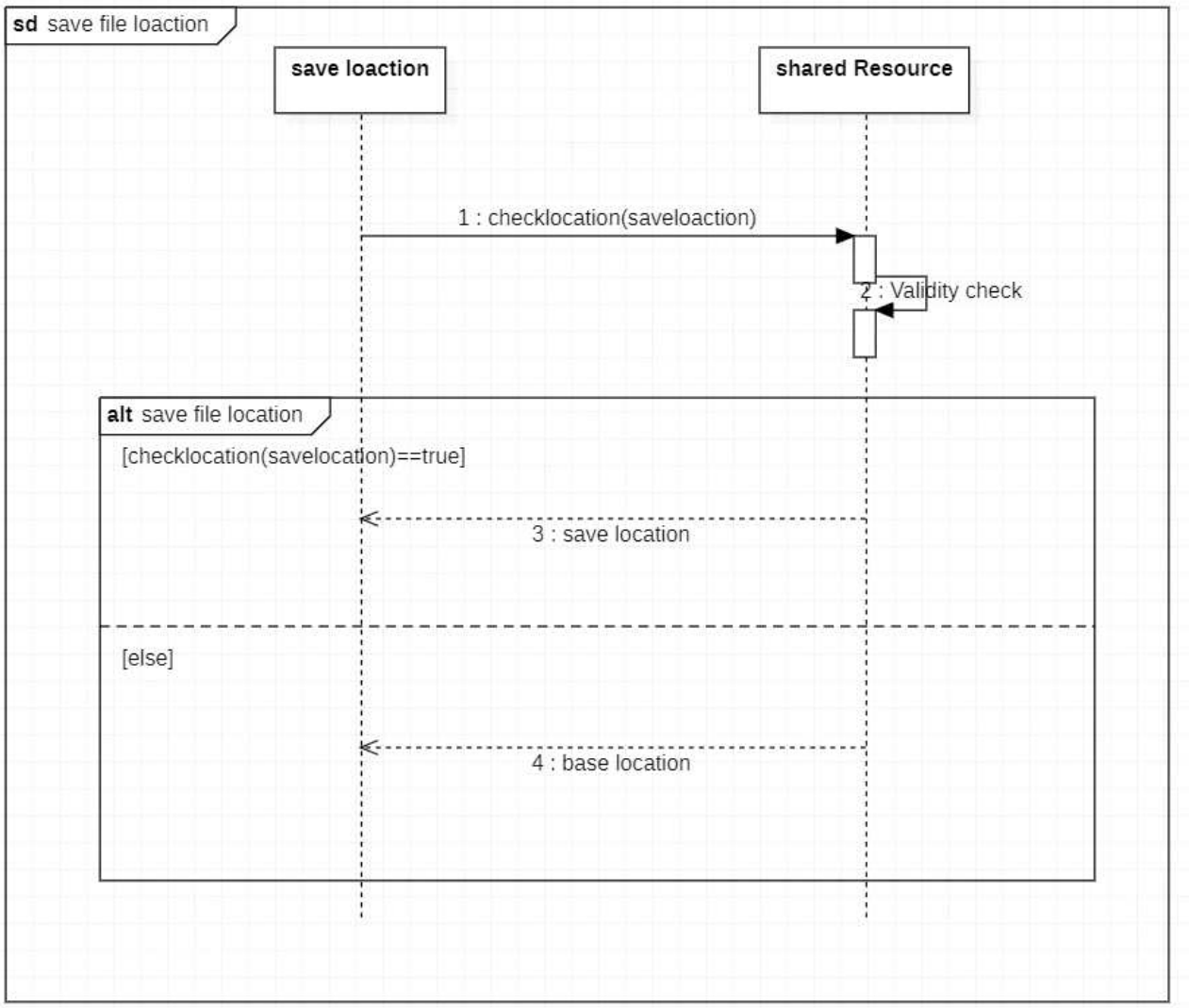
위의 그림은 시스템 실행후 파일 선택 기능을 수행할 때를 표현한 Sequence Diagram 이다. 파일을 선택하여 filecheck 함수를 부른다. 그다음 true로 반환시 select crypto 를 보이게끔 한다.

아래의 그림은 시스템의 기능 중 “Select encryption method“에 대한 Sequence Diagram이다.



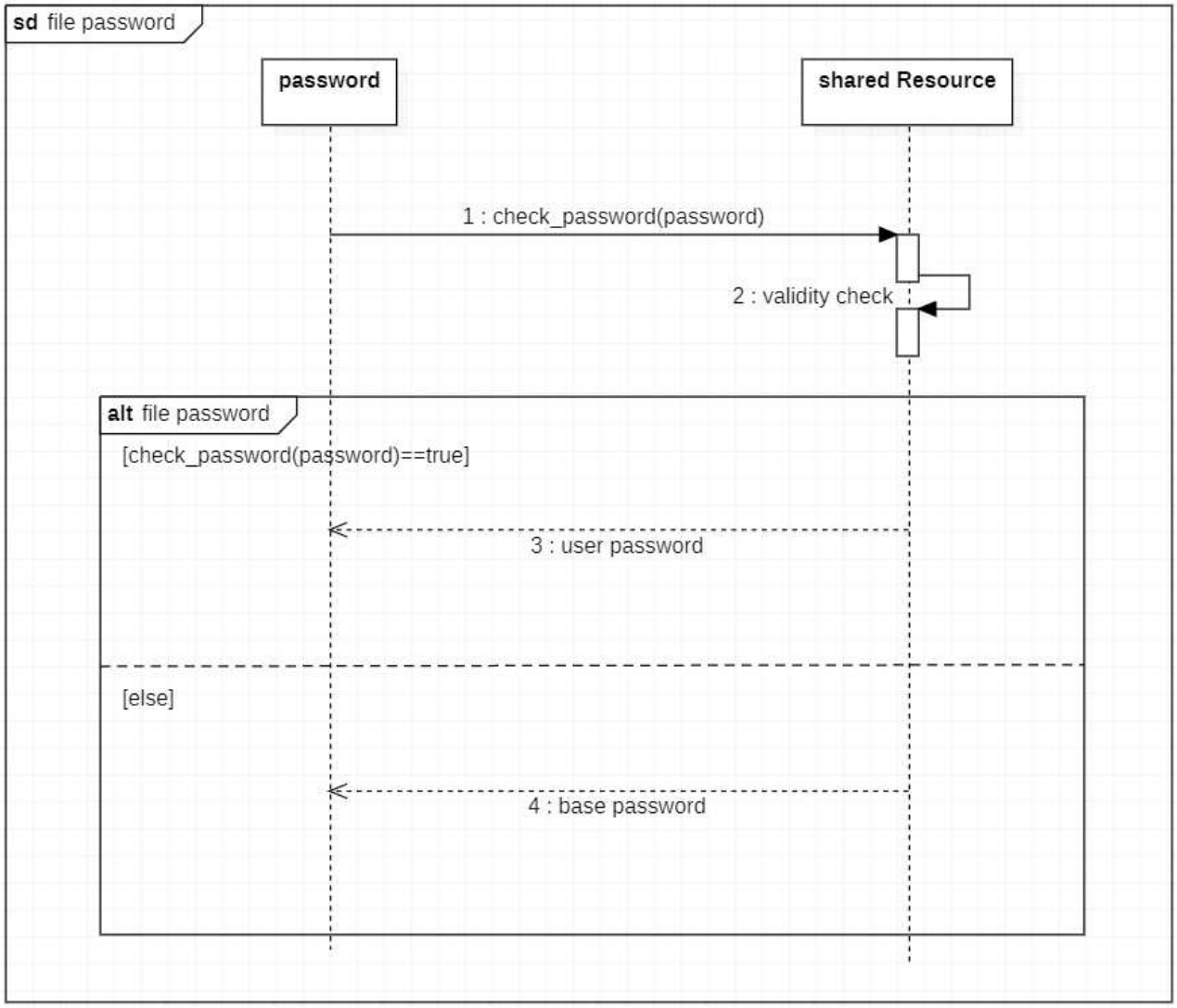
file check에서 true로 반환되었을시 이 기능을 실행하며 암호화/복호화를 선택시 암호화/복호하 기법이 보이며 기법선택시 check encryption()이 ture로 되고 savefile location 기능이 보이게 되며 넘어가게 된다. 기법을 선택안했으면 check encryption() 이 false로 반환되며 ErrorMessage를 출력한다.

아래의 그림은 시스템 기능중 “Save file loaction”에 대한 Sequence Diagram이다.



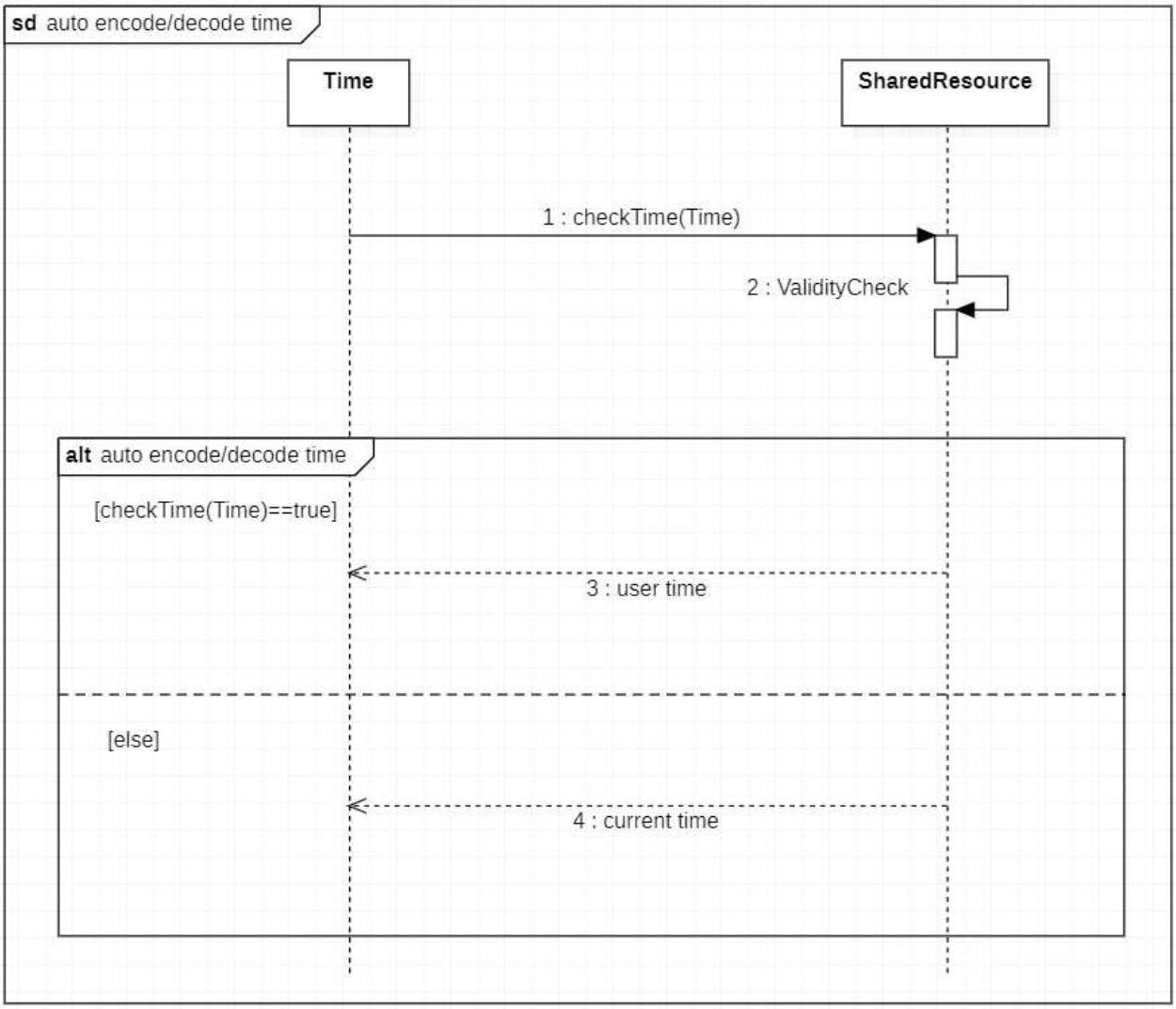
앞서 파일의 암호화 기법을 선택에 성공하였으면 이 기능의 창이 보이며 암호화/복호화된 파일의 저장위치를 설정하였으면 true로 반환하고 true일시 그 위치를 암호화/복호화된 파일의 저장위치로 설정한다. 파일의 저장위치를 설정하지 않아 fasle일시 암호화/복호화 할 파일의 위치에 저장하게 된다.

아래의 그림은 시스템 기능중 “File password”에 대한 Sequence Diagram이다.



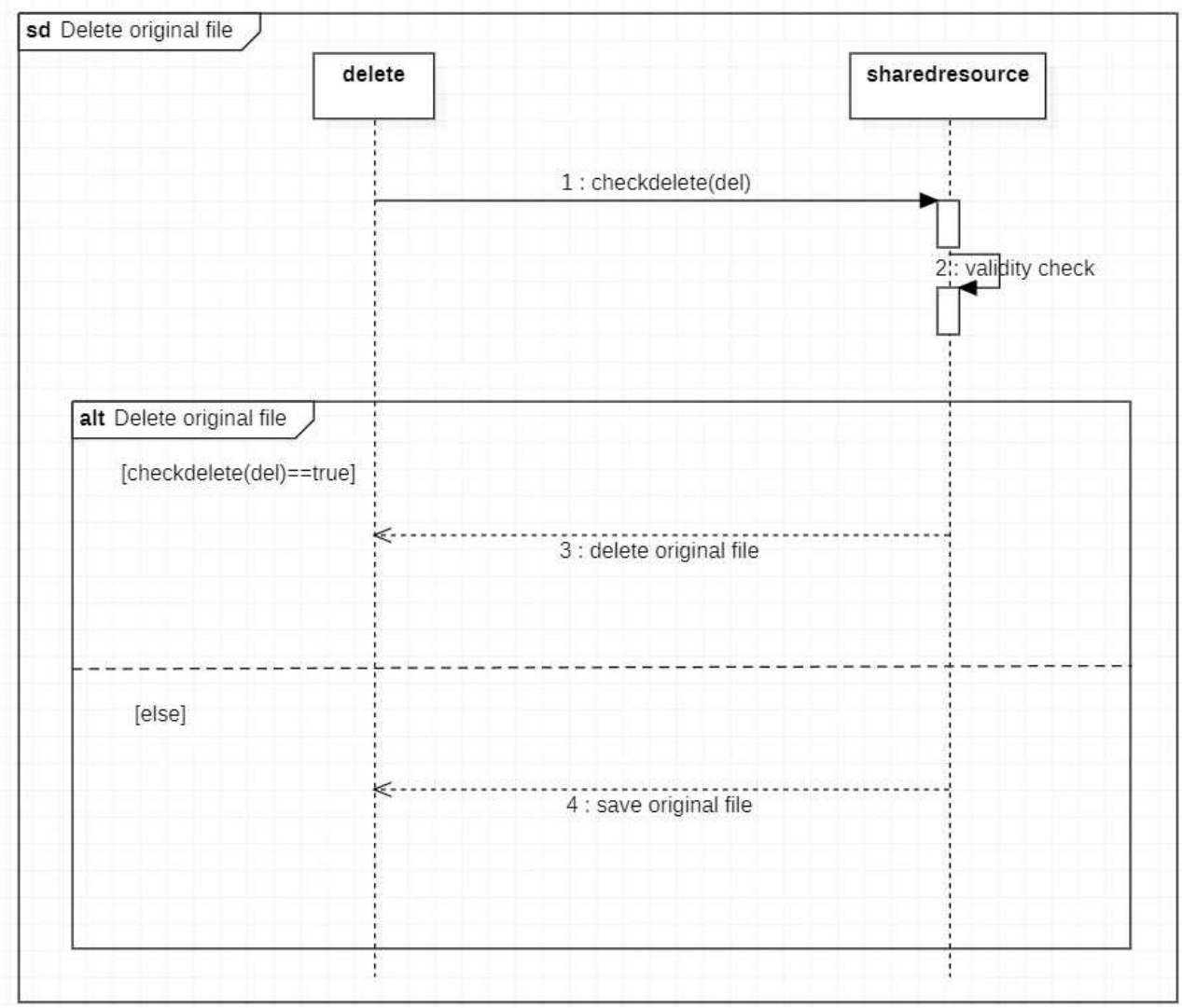
파일을 암호를 입력시 true 미입력시 false로 반환 되며 true일시 유저의 암호를 가져가며 false일시 시스템에서 설정된 기본암호로 암호화/복호화에 사용될 암호로 저장된다.

아래의 그림은 시스템 기능중 “auto encode/decode time”에 대한 Sequence Diagram이다.



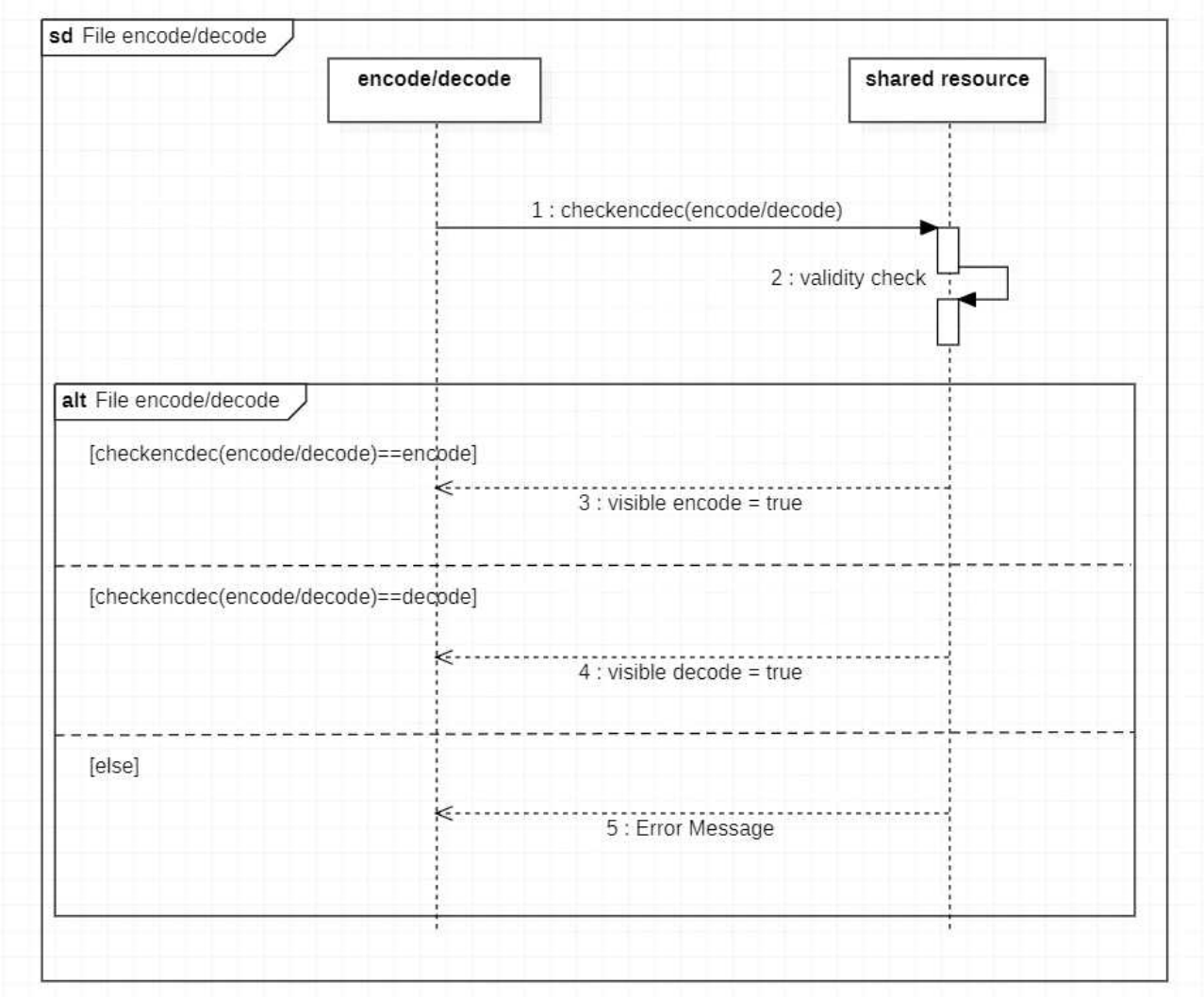
시간을 입력할시 checkTime에 의해 True로 반환이 되며 true시 유저가 입력한 시간이 입력되고 False시 현재시간이 들어가 들어간 시간에 맞게 암호화/복호화가 진행된다.

아래의 그림은 시스템 기능중 “Delete original file”에 대한 Sequence Diagram이다.



Delete를 체크시 기존에 있는 파일을 삭제하고 암호화/복호화된 파일만 남게된다 미체크시 checkdelete에 의해 false값으로 반환되며 기존에 있는 파일을 남겨두게 된다.

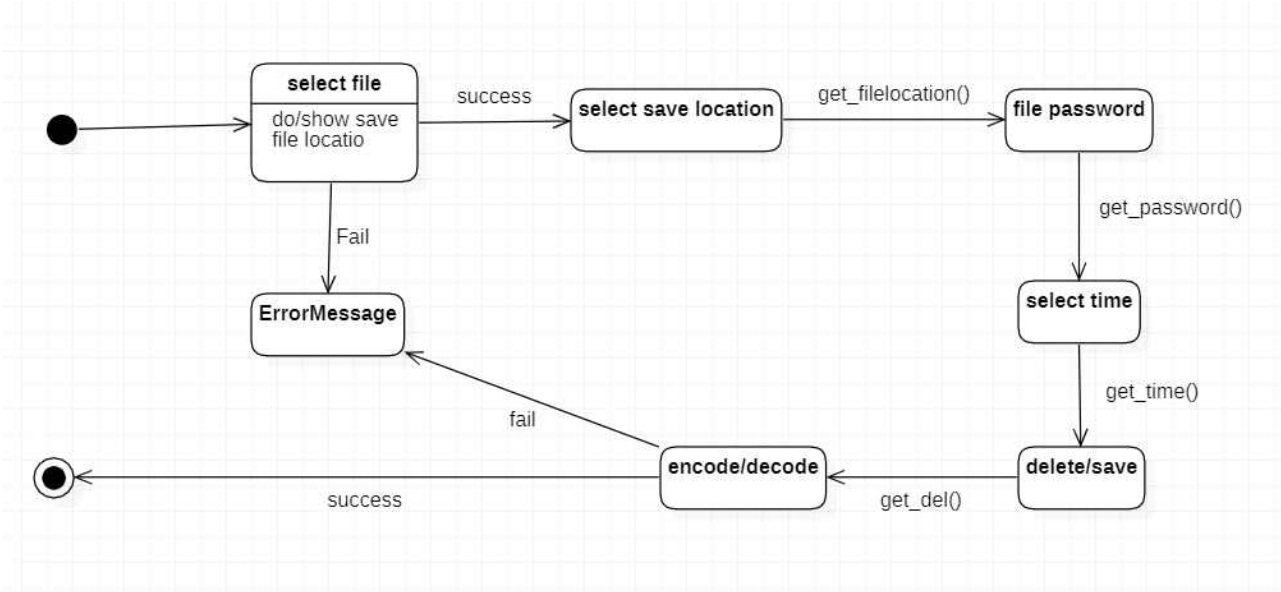
아래의 그림은 시스템 기능중 “File encode/decode”에 대한 Sequence Diagram이다.



encode/decode를 선택하게 되며 encode를 선택시 checkencdec에 의해 encode로 반환되어 암호화 기법 선택창이 보이게 된다. decode를 선택시 decode로 반환되며 복호화 기법선택창이 보이게 된다. 둘다선택하지 않거나 오류가 발생할시 ErrorMessage가 출력된다.

4. State machine diagram

아래의 그림은 save the file's!!시스템의 State machine diagram을 표현한 그림이다.



아래는 위의 State Machine Diagram에 나온 각 State들에 대해서 간단하게 설명한 표이다.

Status	Explanation
select file	파일이 선택하는 상태이다.
select save location	암호화/복호화된 파일의 저장위치를 입력하는 상태를 말한다.
file password	암호화/복호화시 사용할 암호를 입력하는 상태를 말한다.
select time	암호화/복호화를 자동으로 할시간을 입력하거나 미입력으로 즉시 실행되게 입력하는 상태를 말한다.
delete/save	암호화/복호화후 기존의 파일을 삭제할지 저장할지 정하는 상태를 말한다.
encode/deocde	암호화/복호화를 선택후 기법을 선택 및 그 기법으로 암호화/복호화 하는 상태를 말한다.

5. Implementation requirements

save the file's!! 시스템을 구동하기 위해 필요한 요구사항은 아래와 같다.

1)soft ware Requirement

OS – window 7 이상

implementation Language - python

2) Nonfunctional requirements

해당 시스템은 암호화/복호화 기능임으로 일반적인 컴퓨터에서는 다 돌아간다. 암호화 복호화시 암호화 복호화 할 파일이 필요하다.

6. Glossary

암호화 (Encryption): 원래의 데이터를 암호화 알고리즘을 사용하여 암호문으로 변환하는 과정을 말합니다. 암호화된 데이터는 암호키를 알고 있는 사람만이 해독할 수 있습니다.

복호화 (Decryption): 암호문을 암호 해독 알고리즘을 사용하여 원래의 데이터로 변환하는 과정을 말합니다. 암호화된 데이터를 복호화하기 위해서는 암호화 시 사용한 암호키가 필요합니다.

DES (Data Encryption Standard): 암호화 알고리즘 중 하나로, 대칭키 암호화 방식을 사용합니다. DES는 56비트의 암호키를 사용하며, 데이터를 64비트 블록으로 분할하여 암호화합니다. 이 프로그램에서는 DES를 사용하여 암호화 및 복호화를 수행합니다.

AES (Advanced Encryption Standard): 암호화 알고리즘 중 하나로, 대칭키 암호화 방식을 사용합니다. AES는 128비트, 192비트, 256비트의 세 가지 키 길이를 지원하며, 데이터를 블록 단위로 암호화합니다. 이 프로그램에서도 AES를 사용하여 암호화 및 복호화를 수행합니다.

패딩 (Padding): 암호화 알고리즘에서 블록 크기에 맞지 않는 데이터를 처리하기 위해 추가되는 바이트입니다. 패딩은 블록 크기에 맞추어 데이터를 채우는 역할을 수행하며, 복호화 시에는 이를 제거하여 원래 데이터를 복원합니다.

초기화 벡터 (Initialization Vector, IV): 암호화 알고리즘에서 랜덤한 값을 사용하는 초기화 매개 변수입니다. 초기화 벡터는 동일한 키로 여러 블록을 암호화할 때 각 블록을 구분하기 위해 사용됩니다. 암호화와 복호화 시에는 동일한 초기화 벡터를 사용해야 합니다.

스레드 (Thread): 동시에 여러 작업을 수행하기 위해 프로그램 내에서 실행되는 독립적인 실행 흐름입니다. 스레드를 사용하면 여러 작업을 병렬로 처리할 수 있으며, 이 프로그램에서는 일정 시간에 작업을 스케줄링하기 위해 스레드를 사용합니다.

스케줄링 (Scheduling): 작업이 특정 시간에 실행되도록 관리하는 것을 말합니다. 스케줄링은 프로그램의 동작을 제어하여 효율적인 작업 실행을 보장합니다. 이 프로그램에서는 스케줄링을 사용하여 암호화 및 복호화 작업이 일정 시간에 실행되도록 합니다.

7. References

https://gmlwjd9405.github.io/2018/07/04/class-diagram.html
https://steady-hello.tistory.com/132