



데이터 보안 프로그램

DataLoker —

PM 김대형

한국폴리텍 강서캠퍼스 사이버보안과

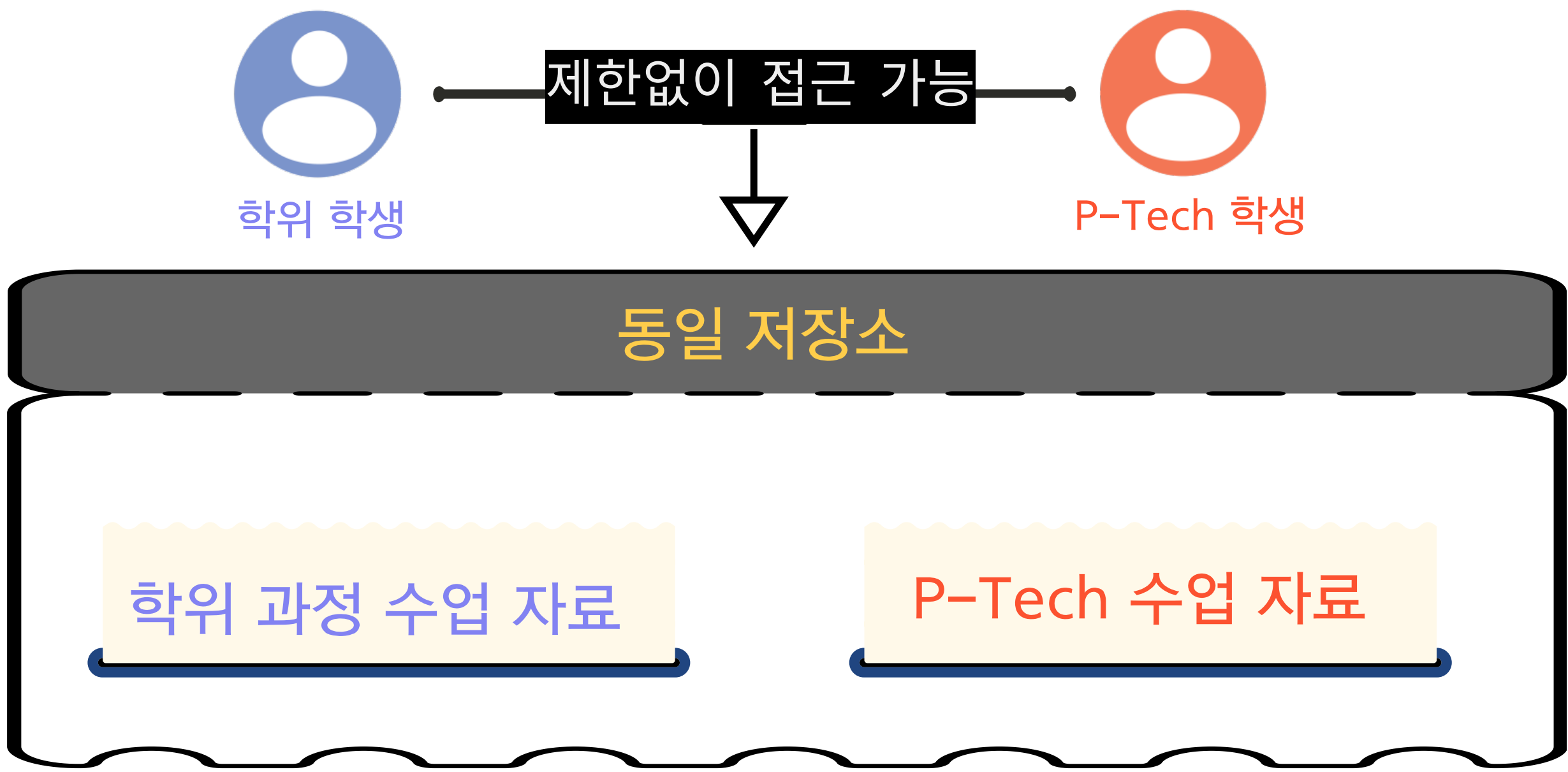


목차

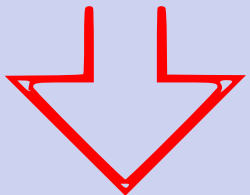
1. 개요
2. 추진 방안
3. 일정 및 조직
4. 결과 시연
5. WBS

추진배경 및 목적

공유 PC 환경에서 개인적 결과물에 대한 무분별한 접근 혹은 수정이 가능한 문제가 발생



상호간 접근을 원천 차단하기 어려운 환경



차선택 : 중요한 데이터의 내용을 암호화



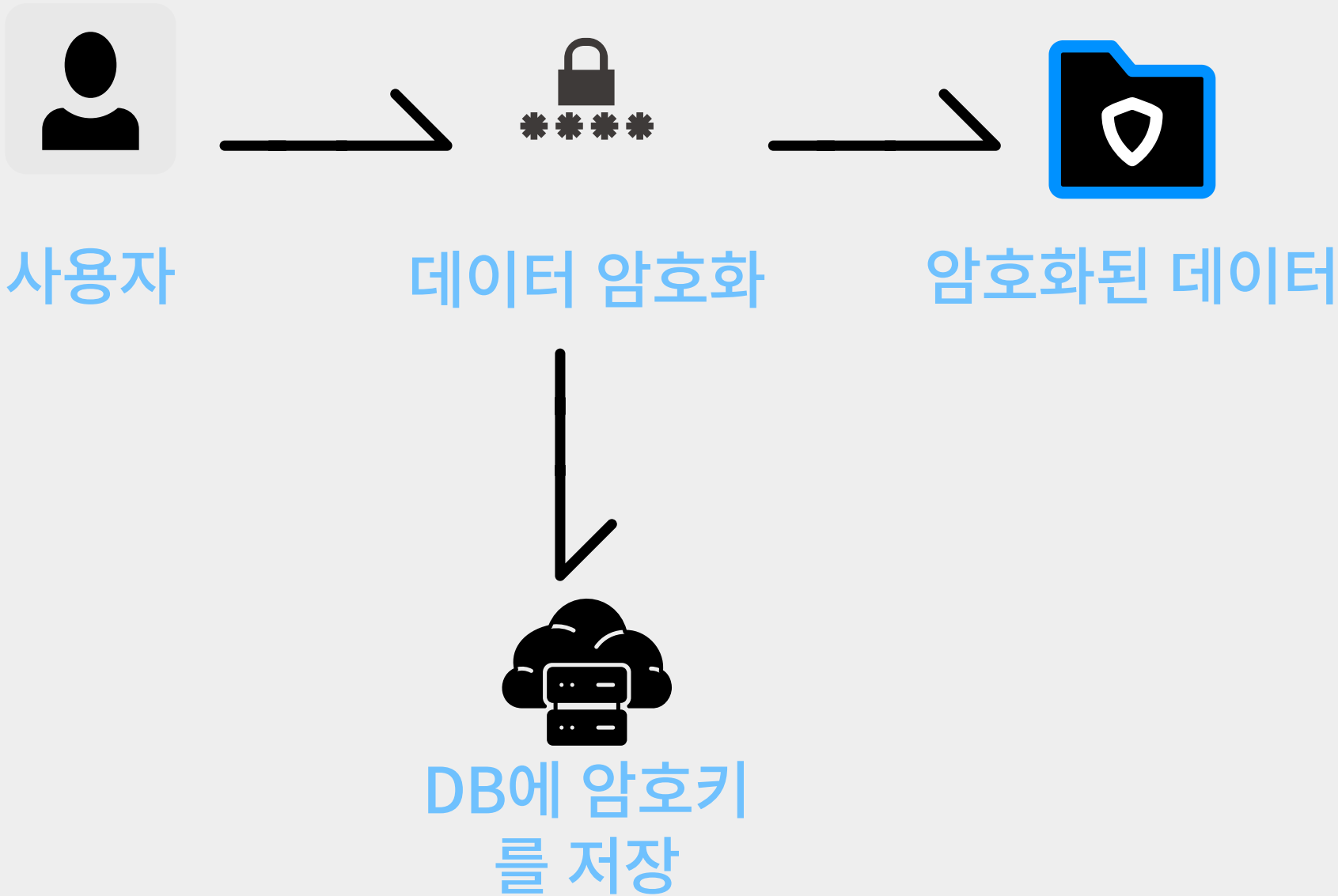
데이터 암호화 프로그램

DataLocker의 필요성

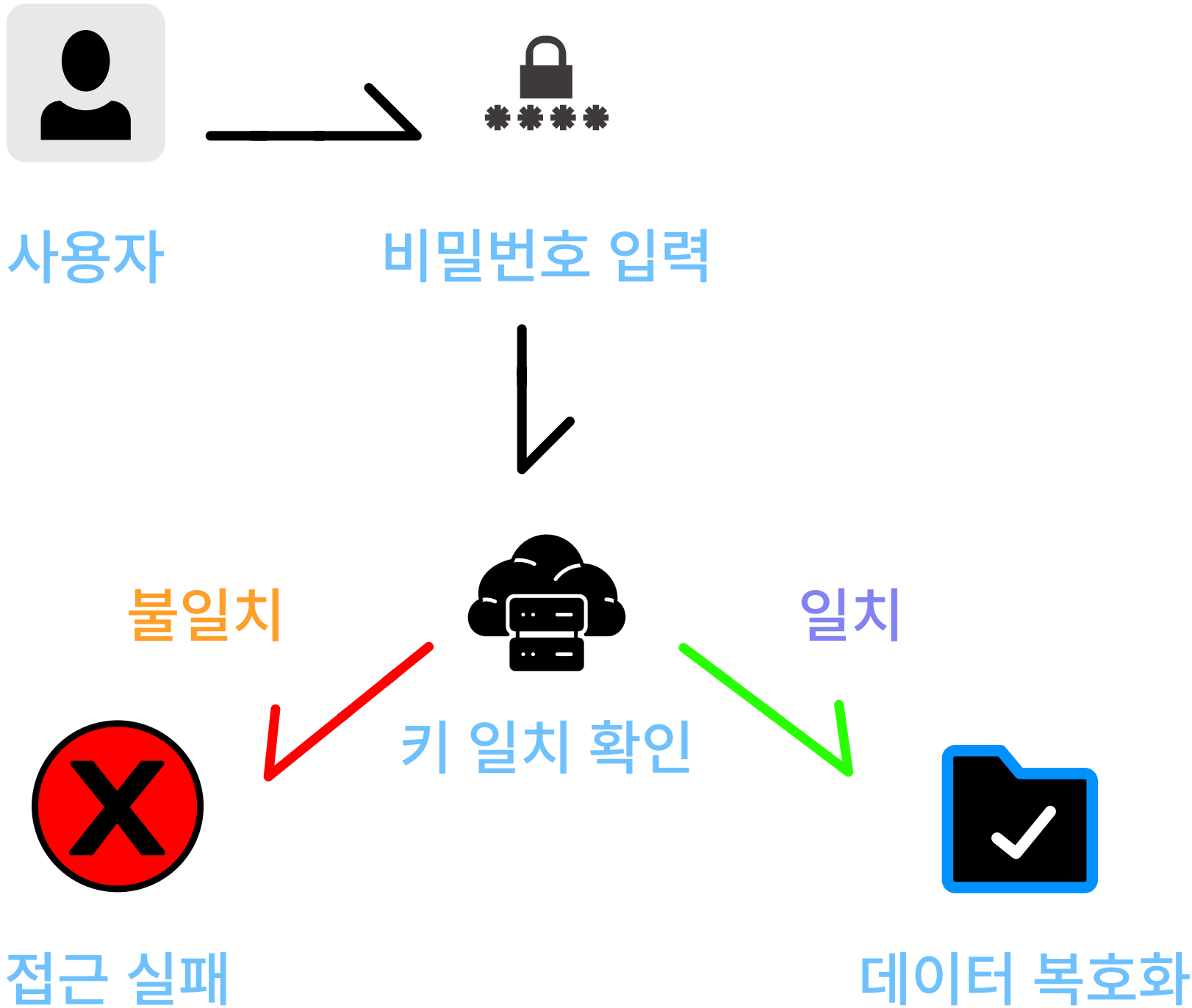
프로젝트 범위

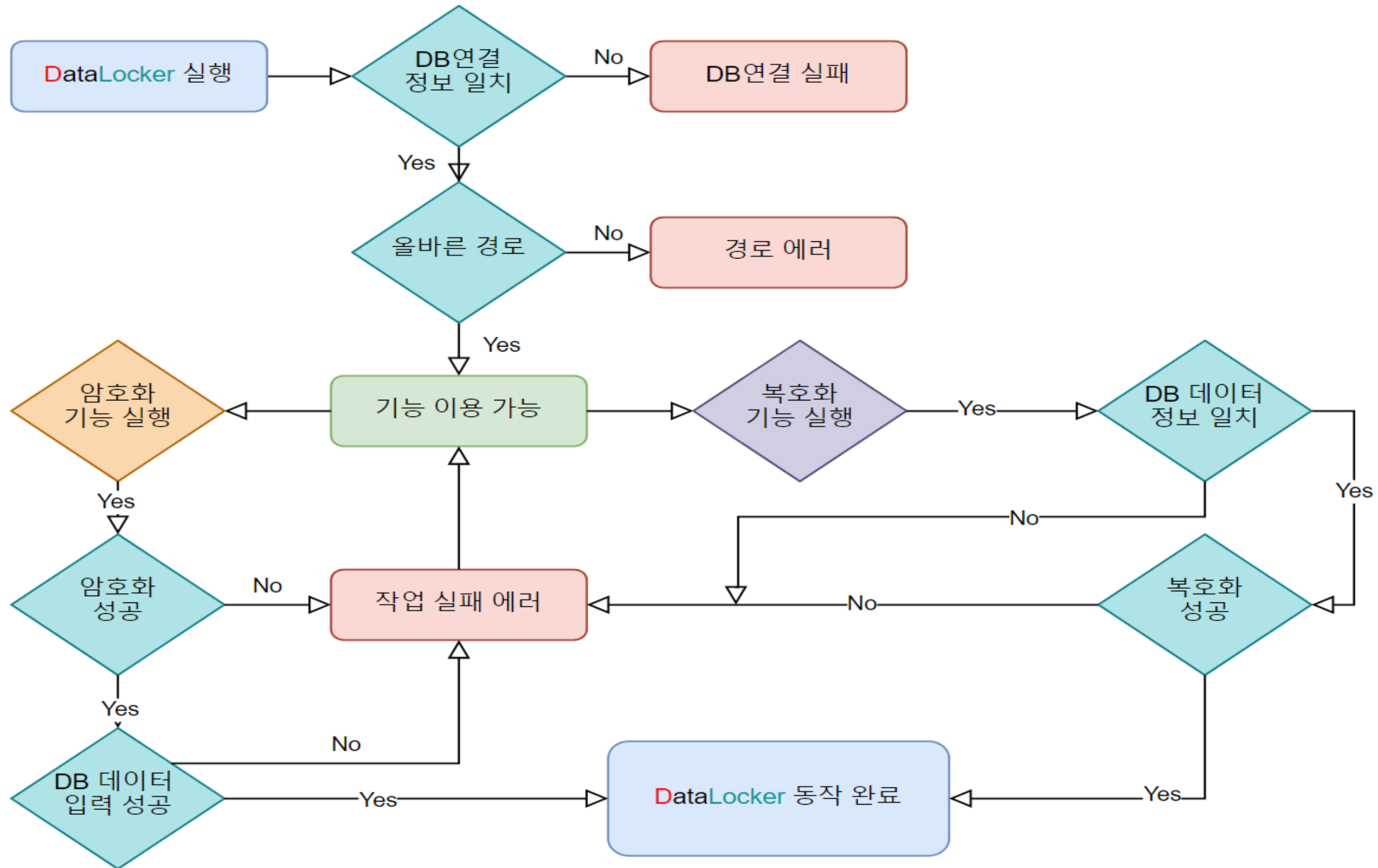
구분	영역	내용	비고
DataLocker 프로젝트	데이터 암호, 복호화 코드	<ul style="list-style-type: none">- DB 접근 정보를 코드 포함 X- 경로 지정 가능- 암호화, 복호화 버튼 별개 구현	- python 활용
	DB 연동	<ul style="list-style-type: none">- 암호화시 경로와 암호화키를 저장- 복호화시 경로 비교 후 암호화키 사용, 작업 후 데이터 삭제	- MYSQL 활용
	로그 생성	<ul style="list-style-type: none">- 암호, 복호화 시도시 로그 작성- 로그는 별도의 테이블에 존재	
	로그 확인용 웹 페이지 구축	<ul style="list-style-type: none">- 암호, 복호화 기능 동작시 경로, 기능, 동작한 시간을 기록- DB 조회 권한이 부여된 별도의 사용자 계정으로 접근	- https, php로 구성하여 TLS 연결

암호화 과정



복호화 과정





시스템 구성

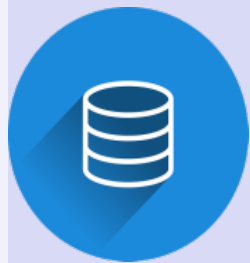
☑ H/W 구성



- 사용자 입력 공간
- 암호화할 파일 위치



- 가상 환경
- https 웹서버
- DB 서버



- 사용자 목록
- 경로, 암호화키
- 로그 내용 기록

☑ S/W 구성



- 암호화 모듈 활용
- UI 구성, 암호화 및 복호화 기능 구현

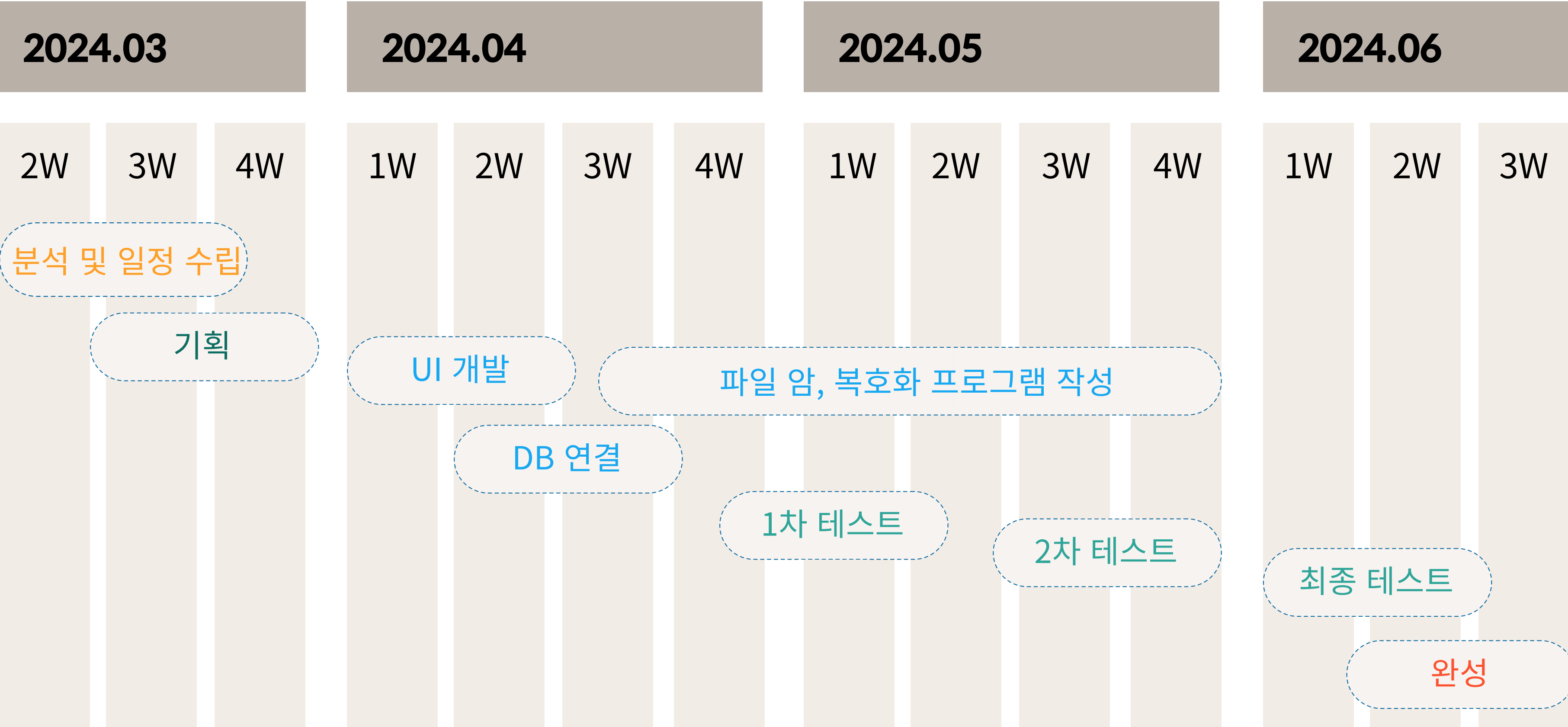
사용 모듈	역할
mysql.connector	MySQL 커넥터
cryptography	AES GCM 암호화



- 파일 경로, 암호키
- 로그 저장

사용 테이블	역할
DLtable	암,복호화 데이터
dl_log	로그

프로젝트 진행 일정



프로젝트 팀 구성

PM 김대형

- 프로젝트 전반의 계획 조정 및 감독
- 잠금 및 해제 프로그래밍 코드 구현, 개발

PL 이명일

- HTTPS 서버 구축
- SSL 환경 구축

PL 이정명

- 암호화 프로그래밍 코드 구현
- WBS 작성

PL 박상헌

- DB 서버 구축

의사소통 방안

구분		의사소통 내용	시기	참석대상
보고	착수보고	- 프로젝트 개요, 수행기간 및 구성 소개 - 추진 방안 및 WBS 협의	24년 4월 8일	평가단(김영희 교수님) 프로젝트 구성원
	중간보고	- 추진계획 대비 결과물 점검 - 주요 이슈 및 해결방안 공유 - 중간 점검 및 향후 진행 방안 보고	24년 4월 29일	평가단(김영희 교수님) 프로젝트 구성원
	완료보고	- 수행 결과 보고 - 결과물 제출, 평가	24년 6월 24일	평가단(김영희 교수님, 안혁 교수님) 프로젝트 구성원
정기회의	주간회의	- 주간 계획 대비 진척 상황 점검 - 이슈 논의 및 해결	매주 월요일	프로젝트 B팀
비정기회의	이슈회의	- 긴급 이슈 사항 공유 - 해결 방안 논의	필요 시, 수시	프로젝트 B팀

최종 결과물

```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
```

```
root@ubuntu:~# mysql --version
mysql Ver 8.0.37-0ubuntu0.20.04.3 for Linux on x86_64 ((Ubuntu))
```

```
tcp6      0      0 :::443          :::*             LISTEN
tcp6      0      0 :::1:631        :::*             LISTEN
tcp6      0      0 :::3306         :::*             LISTEN
```



- https 접속을 위한 openssl 설정
- mysql-server 설치
- 방화벽에서 필요 서비스 허용

```
mysql> show tables;
+-----+
| Tables_in_dl |
+-----+
| DLtable      |
| dl_log       |
+-----+
2 rows in set (0.00 sec)
```

```
mysql> DESC DLtable;
+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| fileID| int           | NO   | PRI | NULL    | auto_increment |
| filepath| varchar(255) | NO   |     | NULL    |                |
| EKey  | varchar(255) | NO   |     | NULL    |                |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)
```

```
mysql> DESC dl_log;
+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id     | int           | NO   | PRI | NULL    | auto_increment |
| filepath| varchar(255) | NO   |     | NULL    |                |
| operation| varchar(255) | NO   |     | NULL    |                |
| timestamp| timestamp    | YES  |     | CURRENT_TIMESTAMP | DEFAULT_GENERATED |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)
```



- 경로, 암호키 저장을 위한 DLtable
- 로그 저장을 위한 dl_log

실행 - DB 연결

- DB 연결을 위한 서버의 IP
- DB user명
- DB user의 비밀번호
- 사용할 DB명

DB 연결을 위한 정보 입력

```
# 데이터베이스 연결 함수
def 데이터베이스에_연결(호스트, 사용자, 비밀번호, 데이터베이스):
    global db_연결, db_커서
    try:
        db_연결 = mysql.connector.connect(
            host=호스트,
            user=사용자,
            password=비밀번호,
            database=데이터베이스
        )
        db_커서 = db_연결.cursor()
        messagebox.showinfo("성공", "데이터베이스에 성공적으로 연결되었습니다.")
        # 사용자 ID 입력 필드, 파일 경로 선택 버튼, 암호화 및 복호화 버튼 프레임 생성
        생성_프레임()
    except mysql.connector.Error as err:
        messagebox.showerror("에러", "DB 정보가 맞지 않습니다.")
```

DataLocker

DB 호스트:

DB 사용자:

DB 비밀번호:

DB 이름:

DB에 연결

4. 결과 시연

DataLocker

DB 호스트: 192.168.17.100

DB 사용자: pm

DB 비밀번호: *****

DB 이름: dl

DB에 연결

성공

i

데이터베이스에 성공적으로 연결되었습니다.

확인

192.168.17.1	192.168.17.100	TCP	66 1485 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
192.168.17.100	192.168.17.1	TCP	66 3306 → 1485 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
192.168.17.1	192.168.17.100	TCP	60 1485 → 3306 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
192.168.17.100	192.168.17.1	MySQL	149 Server Greeting proto=10 version=8.0.37-0ubuntu0.20
192.168.17.1	192.168.17.100	MySQL	90 Login Request user=
192.168.17.100	192.168.17.1	TCP	54 3306 → 1485 [ACK] Seq=96 Ack=37 Win=64256 Len=0
192.168.17.1	192.168.17.100	TLSv1.3	416 Client Hello
192.168.17.100	192.168.17.1	TCP	54 3306 → 1485 [ACK] Seq=96 Ack=399 Win=64128 Len=0
192.168.17.100	192.168.17.1	TLSv1.3	2256 Server Hello, Change Cipher Spec, Application Data,
192.168.17.1	192.168.17.100	TCP	60 1485 → 3306 [ACK] Seq=399 Ack=2298 Win=1051136 Len=
192.168.17.1	192.168.17.100	TLSv1.3	148 Change Cipher Spec, Application Data, Application D
192.168.17.1	192.168.17.100	TLSv1.3	389 Application Data
192.168.17.100	192.168.17.1	TLSv1.3	293 Application Data
192.168.17.100	192.168.17.1	TLSv1.3	293 Application Data

Transport Layer Security

▼ TLSv1.3 Record Layer: Application Data Protocol: mysql

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

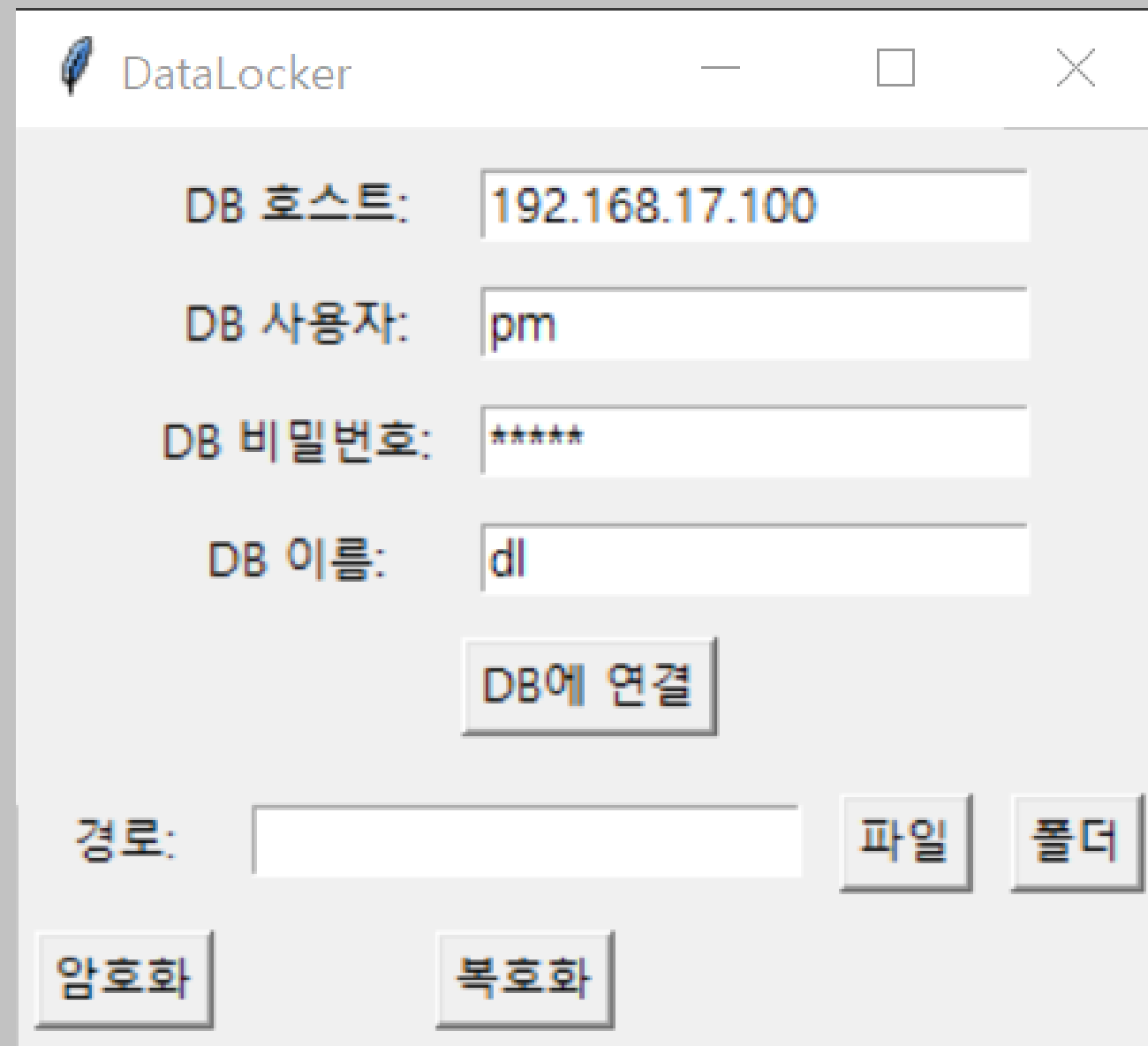
Length: 41

Encrypted Application Data: b6a87d6f9d106392002f949a1ed3a837942371e86017dff6...

000	00 0c 29 20 f6 14 00 50	56 c0 00 08 08 00 45 00	..) ...P V.....E.
010	00 56 28 72 40 00 80 06	2e 7a c0 a8 11 01 c0 a8	.V(r@... .z.....
020	11 64 05 cd 0c ea 0a 61	aa 12 87 b3 5a 76 50 18	.d.....aZvP.
030	10 08 c0 c2 00 00 17 03	03 00 29 b6 a8 7d 6f 9d)..}o.
040	10 63 92 00 2f 94 9a 1e	d3 a8 37 94 23 71 e8 60	.c../... ..7.#q.`
050	17 df f6 3d 8f 16 5d 43	25 d5 74 b2 45 85 d5 4f	...=..]C %.t.E..0
060	57 11 ab ea		W...

DB 연결 정보가 맞다면 연결 성공

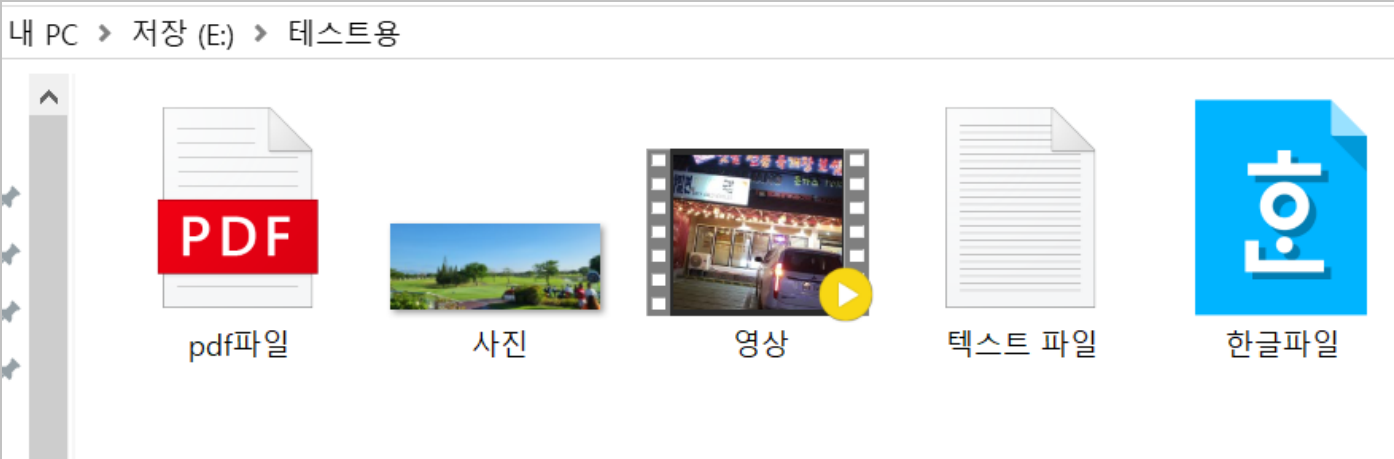
4. 결과 시연



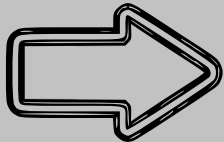
The screenshot shows the DataLocker application window. It has a title bar with the icon and text 'DataLocker'. The main area contains four input fields with labels: 'DB 호스트:' with the value '192.168.17.100', 'DB 사용자:' with the value 'pm', 'DB 비밀번호:' with the value '*****', and 'DB 이름:' with the value 'dl'. Below these fields is a button labeled 'DB에 연결'. At the bottom, there is a '경로:' label followed by an empty text box, and two buttons labeled '파일' and '폴더'. In the bottom left corner, there are two buttons labeled '암호화' and '복호화'.

- DB 연결에 성공하면 경로 선택
- 개별 파일 혹은 폴더 모두 가능
- 경로 선택 후 기능 버튼 사용

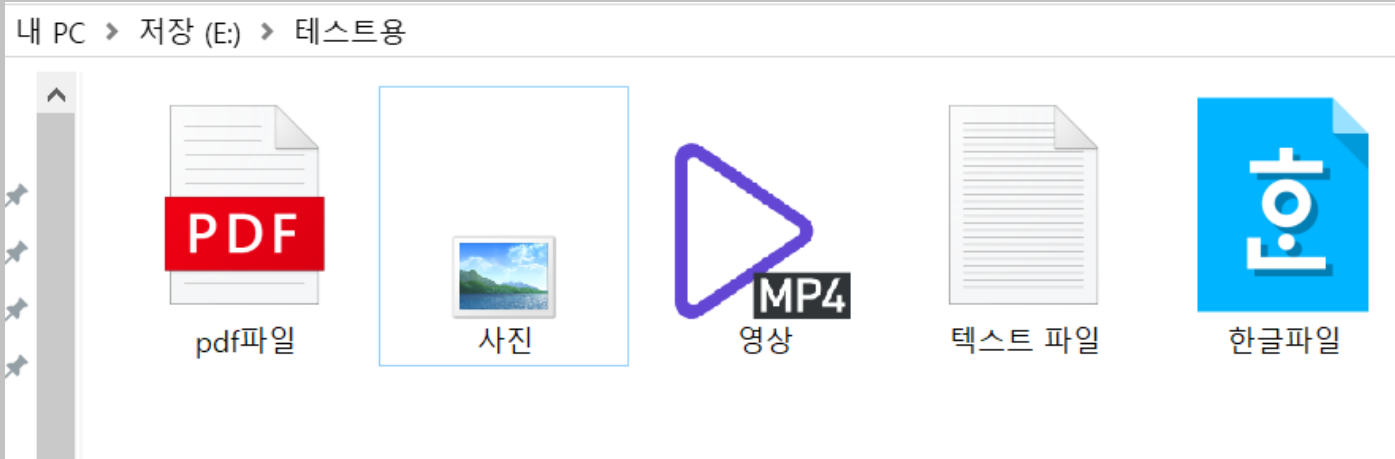
4. 결과 시연



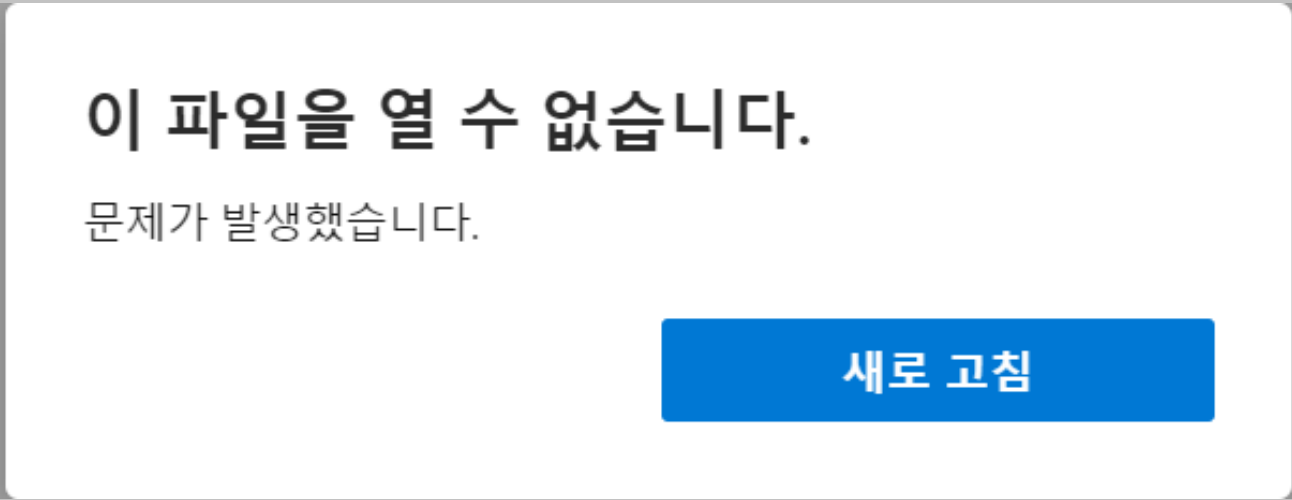
암호화 이전 원본



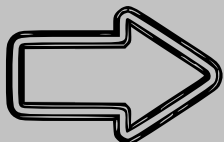
데이터로커 암호화



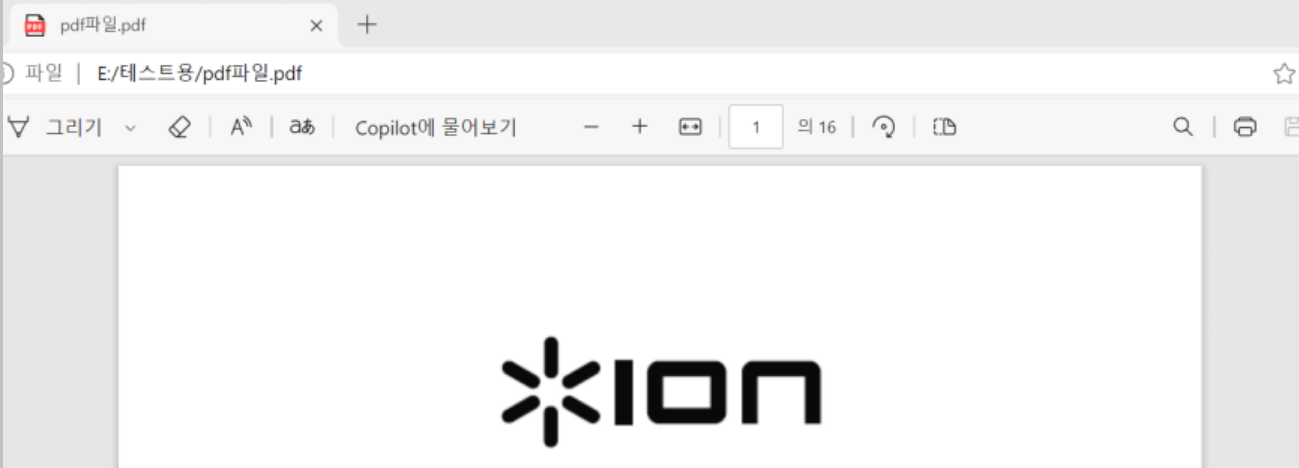
내용 변경 및 실행 불가



암호화 파일 내용 확인 불가



데이터로커 복호화



복호화 후 내용 확인

데이터의 암호, 복호화 구현 성공


```
mysql> select * from DLtable;
```

fileID	filepath	EKey
1	E:/테스트용/pdf파일.pdf	yIUR-J894w35KiRpgYeP2F0hQWjEowSPA3MjH40f28g=
2	E:/테스트용/사진.jpg	g85YBGW79mjMvHWjgxTcfHdpHEqvphNRzG9C77CHCWk=
3	E:/테스트용/영상.mp4	Yaah4x3X3wYKjMtKy94t6pybCRtipmWfgYYiJR8lLsg=
4	E:/테스트용/텍스트 파일.txt	in6dmcNRhqWHBeK_uPvcA2S5IBd87C9fTVmMU1VkTg0=
5	E:/테스트용/한글파일.hwp	qGAJSazx3nuMj48b5k6mGigr00DfniVfHJKm5ZQEx8A=

5 rows in set (0.00 sec)

```
mysql> select * from dl_log;
```

id	filepath	operation	timestamp
1	E:/테스트용/pdf파일.pdf	encryption activated	2024-06-22 13:49:57
2	E:/테스트용/사진.jpg	encryption activated	2024-06-22 13:50:00
3	E:/테스트용/영상.mp4	encryption activated	2024-06-22 13:50:02
4	E:/테스트용/텍스트 파일.txt	encryption activated	2024-06-22 13:50:05
5	E:/테스트용/한글파일.hwp	encryption activated	2024-06-22 13:50:08

5 rows in set (0.00 sec)

암호화 기능 사용 시

DLtable에
데이터들의 경로,
암호화키가 저장

dl_log에
동작, 시간 저장

```
mysql> select * from DLtable;
+-----+-----+-----+
| fileID | filepath                | EKey                |
+-----+-----+-----+
| 3      | E:/테스트용/영상.mp4    | Yaah4x3X3wYKjMtKy94t6pybCRtipmWfgYYiJR8lLsg= |
| 4      | E:/테스트용/텍스트 파일.txt | in6dmcNRhqWHBeK_uPvcA2S5IBd87C9fTVmMU1VkTg0= |
| 5      | E:/테스트용/한글파일.hwp | qGAJSazx3nuMj48b5k6mGigr00DfniVfHJKm5ZQEx8A= |
+-----+-----+-----+
3 rows in set (0.00 sec)
```

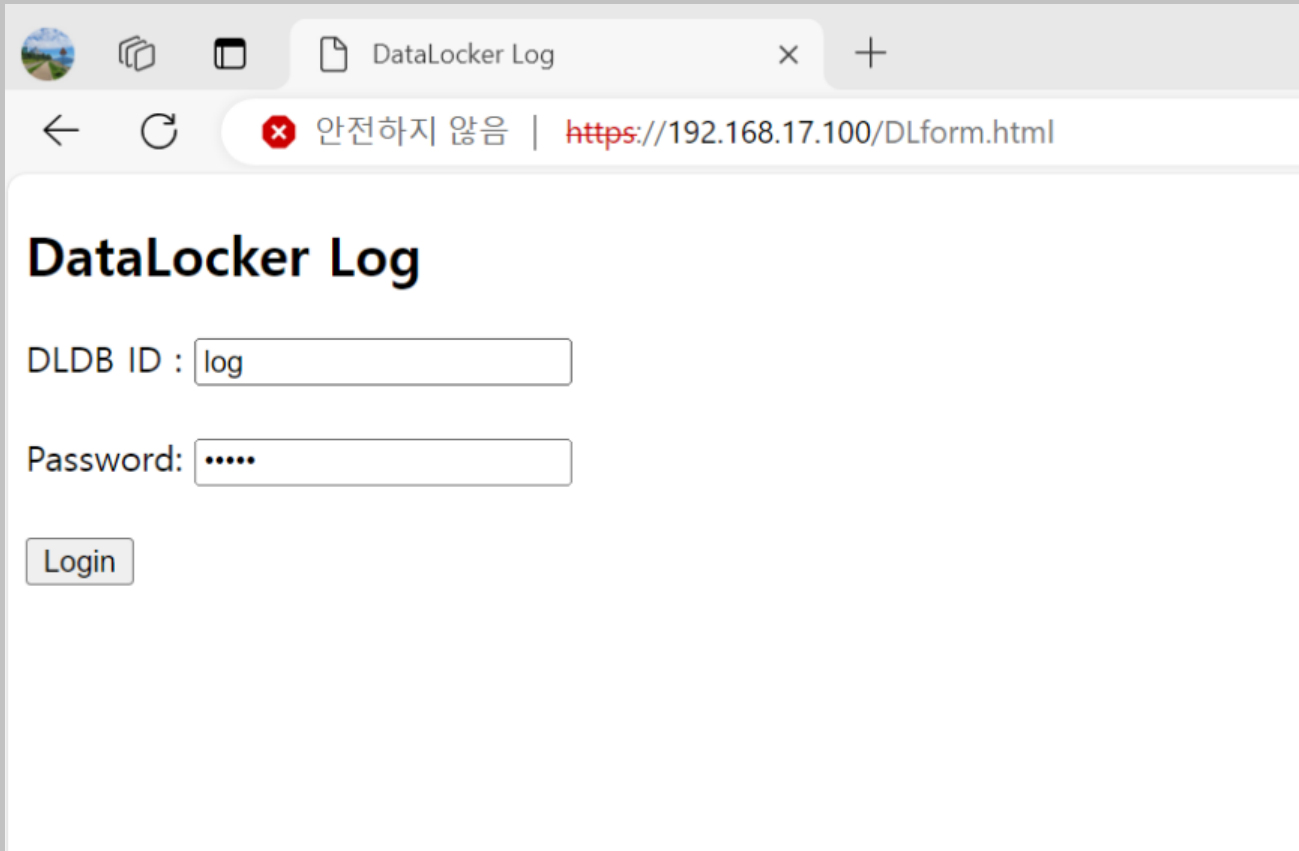
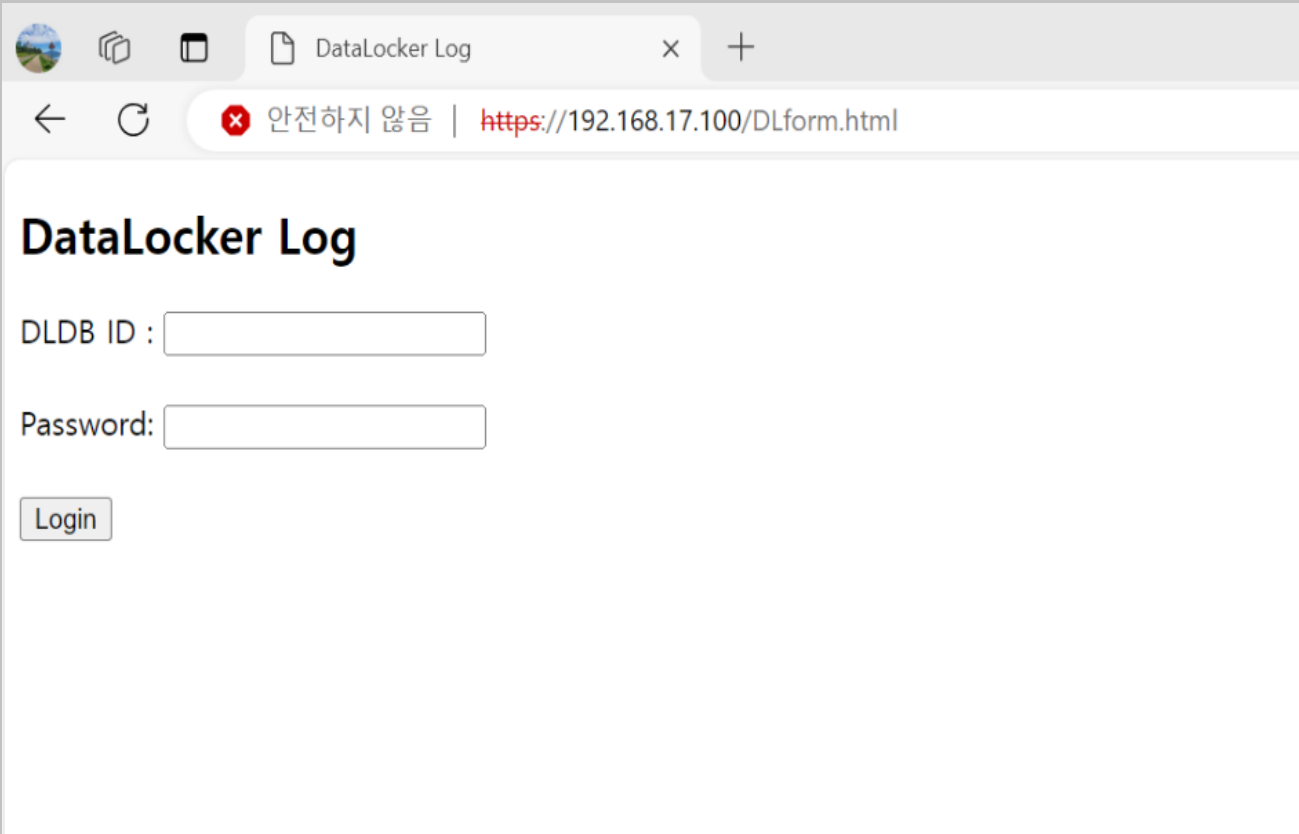
```
mysql> select * from dl_log;
+-----+-----+-----+-----+
| id | filepath                | operation            | timestamp            |
+-----+-----+-----+-----+
| 1  | E:/테스트용/pdf파일.pdf | encryption activated | 2024-06-22 13:49:57 |
| 2  | E:/테스트용/사진.jpg    | encryption activated | 2024-06-22 13:50:00 |
| 3  | E:/테스트용/영상.mp4    | encryption activated | 2024-06-22 13:50:02 |
| 4  | E:/테스트용/텍스트 파일.txt | encryption activated | 2024-06-22 13:50:05 |
| 5  | E:/테스트용/한글파일.hwp | encryption activated | 2024-06-22 13:50:08 |
| 6  | E:/테스트용/pdf파일.pdf | decryption activated | 2024-06-22 13:51:31 |
| 7  | E:/테스트용/사진.jpg    | decryption activated | 2024-06-22 13:51:34 |
+-----+-----+-----+-----+
7 rows in set (0.00 sec)
```

복호화 기능 사용 시

DLtable의
데이터로 복호화 후
사용한 데이터 삭제

dl_log에
동작, 시간 저장

4. 결과 시연



192.168.17.1	192.168.17.100	TCP	66 3065 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
192.168.17.100	192.168.17.1	TCP	66 443 → 3065 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
192.168.17.1	192.168.17.100	TCP	60 3065 → 443 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
192.168.17.1	192.168.17.100	TLSv1.3	1819 Client Hello
192.168.17.100	192.168.17.1	TCP	54 443 → 3065 [ACK] Seq=1 Ack=1766 Win=63488 Len=0
192.168.17.100	192.168.17.1	TLSv1.3	1420 Server Hello, Change Cipher Spec, Application Data,
192.168.17.1	192.168.17.100	TLSv1.3	118 Change Cipher Spec, Application Data
192.168.17.1	192.168.17.100	TLSv1.3	975 Application Data
192.168.17.100	192.168.17.1	TLSv1.3	325 Application Data
192.168.17.100	192.168.17.1	TLSv1.3	325 Application Data
192.168.17.1	192.168.17.100	TCP	60 3065 → 443 [ACK] Seq=2751 Ack=1909 Win=1051136 Len=
192.168.17.100	192.168.17.1	TLSv1.3	656 Application Data
192.168.17.1	192.168.17.100	TCP	60 3065 → 443 [ACK] Seq=2751 Ack=2511 Win=1050368 Len=

[Time since previous frame in this TCP stream: 0.000047379 seconds]

TCP payload (921 bytes)

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 916

Encrypted Application Data: 623e360a83bdfb2856c70e4dd6a18c693292cf3708498488...

0030	10 04 59 55 00 00 17 03 03 03 94	62 3e 36 0a 83	..YU....b>6..
0040	bd fb 28 56 c7 0e 4d d6 a1 8c 69 32 92 cf 37 08		..(V..M. ..i2..7.
0050	49 84 88 45 eb 74 e1 56 fc f2 63 bd 24 56 95 cc		I..E.t.V ..c.\$V..
0060	26 f3 1d d8 08 b2 87 cb c8 8f db e0 20 59 2a c4		&..... Y*.
0070	9d ea b9 6a 06 54 c9 f5 e5 1a 78 9f 2f 64 a6 79		...j.T.. ..x./d.y
0080	87 2c c3 84 6a 5d bf 5e ce e7 f8 c0 7e f7 d8 ae		.,..j].^~...
0090	66 51 7d d2 13 7e 89 a1 c6 88 a3 82 c0 75 1b ec		fQ}...~... ..u..
00a0	2a 3f f6 73 5d b2 89 9c a8 79 6a 03 a0 1e 0f 2b		*?.s]... .yj....+
00b0	ac b1 6a 86 87 54 10 63 d2 a7 2f fa 6d 73 dc 9f		..j..T.c ../.ms..
00c0	74 6e 1e f4 9f 06 7f 94 d3 3a 33 2d 10 51 af 16		tn..... :3-..Q..
00d0	86 0d e7 1e 85 e4 41 ad b4 0c 54 62 56 3c da 5a	A. ..TbV<..Z
00e0	a6 bf dc 35 54 b8 a0 99 fe b2 a0 8d 83 56 4a 16		...5T...VJ.

4. 결과 시연

192.168.17.100/check.php

×

+

←

↺

⛔ 안전하지 않음 | https://192.168.17.100/check.php

DataLocker Log:

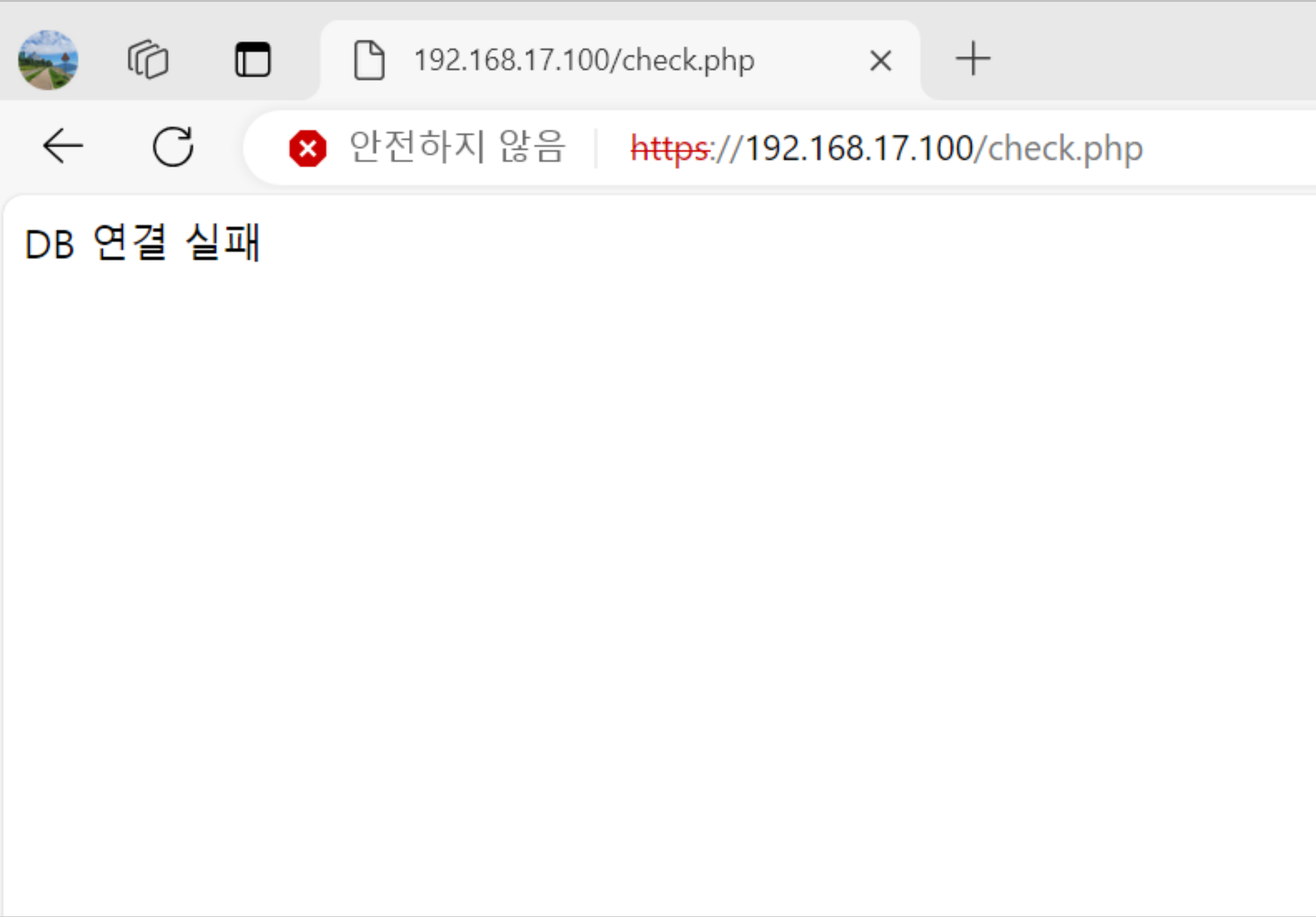
filepath	operation	timestamp
E:/테스트용/pdf파일.pdf	encryption activated	2024-06-22 13:49:57
E:/테스트용/사진.jpg	encryption activated	2024-06-22 13:50:00
E:/테스트용/영상.mp4	encryption activated	2024-06-22 13:50:02
E:/테스트용/텍스트 파일.txt	encryption activated	2024-06-22 13:50:05
E:/테스트용/한글파일.hwp	encryption activated	2024-06-22 13:50:08
E:/테스트용/pdf파일.pdf	decryption activated	2024-06-22 13:51:31
E:/테스트용/사진.jpg	decryption activated	2024-06-22 13:51:34
E:/테스트용/영상.mp4	decryption activated	2024-06-22 13:52:35
E:/테스트용/텍스트 파일.txt	decryption activated	2024-06-22 13:52:38
E:/테스트용/한글파일.hwp	decryption activated	2024-06-22 13:52:40

DB 로그 확인

DLform.html에
관리자 계정으로 접속

외부에서 로그 확인

4. 결과 시연



DB 로그 확인

정당한 사용자가 아닐
경우 연결 실패

DataLocker WBS

WBS		프로젝트 명	데이터 암호화 시스템 (DataLocker)		프로젝트 참여자	
작성자	이정명	작성일	2024년 3월 11일		PM	김대형
부 작성자	김대형	최종 수정일	2024년 6월 22일		PL	박상헌
시작일	2024년 3월 11일	버전	WBS v3.3		PL	이명일
종료일	2024년 6월 24일				PL	이정명

단계 구분	주요 업무	세부 업무	작업자	산출물	수행						M W D
					상태	진척율(%)	진척도(10)	시작일	종료일	작업기간	
주요 MileStone	보고	착수 보고	공통	수행계획서				2024-04-08	2024-04-08		
		중간 보고	공통	중간보고서(&WBS)				2024-04-29	2024-04-29		
		최종 보고	공통	수행결과보고서				2024-06-24	2024-06-24		
1. 준비	1.1 분석	1.1.1 보안 추세 확인	공통	프로젝트제안서 WBS	완료	100%	10	2024-03-11	2024-03-14	4일	
		1.1.2 프로젝트 일정 수립	공통		완료	100%	10	2024-03-15	2024-03-19	5일	
2. 설계	2.1 기획	2.1.1 UI, DB 설계	공통	수행계획서	완료	100%	10	2024-03-18	2024-03-29	12일	
		2.1.2 암호화 알고리즘 선택	공통	수행계획서	완료	100%	10	2024-03-21	2024-03-27	7일	
3. 개발	3.1 웹서버구축	3.1.1 SSL 환경구축	이명일	SSL 연결 가능	완료	100%	10	2024-03-25	2024-04-04	11일	
		3.1.2 UI 디자인 조정	이명일	입력 화면(개선)	완료	100%	10	2024-03-29	2024-04-05	8일	
		3.1.3 HTTPS 페이지 구축	이명일, 박상헌	HTTPS 웹페이지	완료	100%	10	2024-04-18	2024-05-10	23일	
	3.2 DB 연동 구현	3.2.1 DB 접근 제어 및 조회 구현	박상헌	DB 시험 결과	완료	100%	10	2024-04-05	2024-04-12	8일	
		3.2.2 SQL 연결 구현	박상헌, 이명일	주 DB	완료	100%	10	2024-05-21	2024-05-31	11일	
	3.3 주 프로그래밍 코드 작성	3.3.1 파일 암호화 구현	김대형, 이정명	데이터 암호화 모듈	완료	100%	10	2024-04-01	2024-06-10	71일	
		3.3.2 기능 로그 기록 구현	김대형, 이정명	로그 기록 모듈	완료	100%	10	2024-06-03	2024-06-13	11일	
		3.3.3 각 모듈 통합 구축	공통	DataLocker 프로토타입	완료	100%	10	2024-05-28	2024-06-14	18일	
4. 검수	4.1 테스트 및 리뷰	4.1.1 1차 테스트(3.3.1)	공통	1차 테스트 보고서	완료	100%	10	2024-04-29	2024-05-10	12일	
		4.1.2 피드백 및 오류수정 (1차)	공통	(결함/오류 보고서)	완료	100%	10	2024-04-29	2024-05-10	12일	
		4.2.1 2차 테스트(3.3.2)	공통	2차 테스트 보고서	완료	100%	10	2024-05-21	2024-05-31	11일	
		4.2.2 피드백 및 오류수정 (2차)	공통	(결함/오류 보고서)	완료	100%	10	2024-05-21	2024-05-31	11일	
		4.3.1 최종 테스트	공통	최종 테스트 보고서	완료	100%	10	2024-06-14	2024-06-14	1일	
5. 완료	5.1 배포	5.1.1 배포		DataLocker ver 1.0.0	완료	100%	10	2024-06-24	2024-06-24	1일	



감사합니다

