Assignment #2

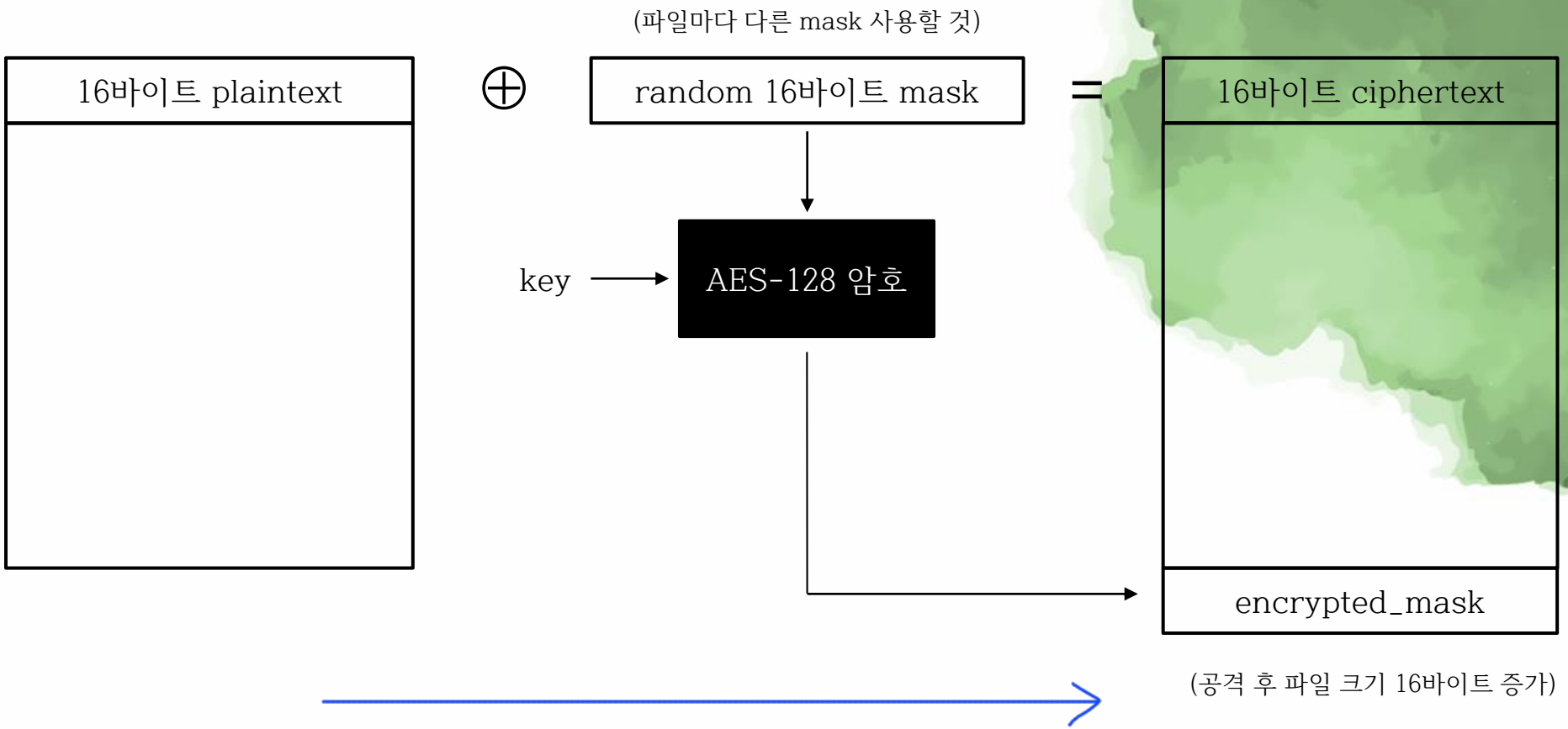
- 멀티스레딩으로 랜섬웨어 구현하기 (공격)
- ./dkuware attack "password" 공격자의 비밀키
  - 2개의 스레드 생성 : 각각 target 폴더 아래 있는 PDF 파일들과 JPG 파일들을 조회 (스레드마다 공격 대상 파일 타입 분리)
  - 대상 파일마다
    - 첫 16바이트 추출 (plaintext)
    - 16바이트 랜덤값 (mask) 생성하여 plaintext와 XOR (ciphertext = plaintext xor mask)
    - 파일의 첫 16바이트를 ciphertext로 overwrite
    - 세번째 인자인 "password" 에서 16바이트를 추출하여 unsigned char의 배열로 저장 (key)
    - Openssl 내 AES-128 암호 알고리즘을 이용하여 상기 mask 를 key로 암호화 (encrypted_mask)
    - 대상 파일의 끝에 encrypted_mask를 append
    - 암호화 중임을 알리는 메시지 출력 ([attack] 파일명)
  - 총 몇 개의 PDF 파일 / 몇 개의 JGP 파일이 공격되었는지 알리는 메시지 출력
  - 모든 대상 파일들 암호화 후에는 ransom note 출력 (제공)

Assignment #2

- 멀티스레딩으로 랜섬웨어 구현하기 (복원)
- ./dkuware restore "password" 공격자의 비밀키
  - 2개의 스레드 생성 : 각각 target 폴더 아래 있는 손상된 PDF 파일들과 JPG 파일들을 조회
  - 대상 파일마다
    - 첫 16바이트 추출 (ciphertext)
    - 마지막 16바이트 추출 (encrypted_mask)
    - Openssl 내 AES-128 복호 알고리즘을 이용하여 encrypted_mask 를 key로 복호화 (mask)
    - 상기 mask를 이용하여 파일의 정상 16 바이트를 찾음 (plaintext = ciphertext xor mask)
    - 파일의 첫 16바이트를 복원하기 위해 plaintext로 overwrite
    - 대상 파일의 마지막 16바이트를 삭제하여 원본 파일로 복원
    - 복원 중임을 알리는 메시지 출력 ([restore] 파일명)
  - 총 몇 개의 PDF 파일 / 몇 개의 JGP 파일이 복원되었는지 알리는 메시지 출력
  - 모든 대상 파일들 복원한 후에는 정상 복구를 알리는 note 출력 (제공)

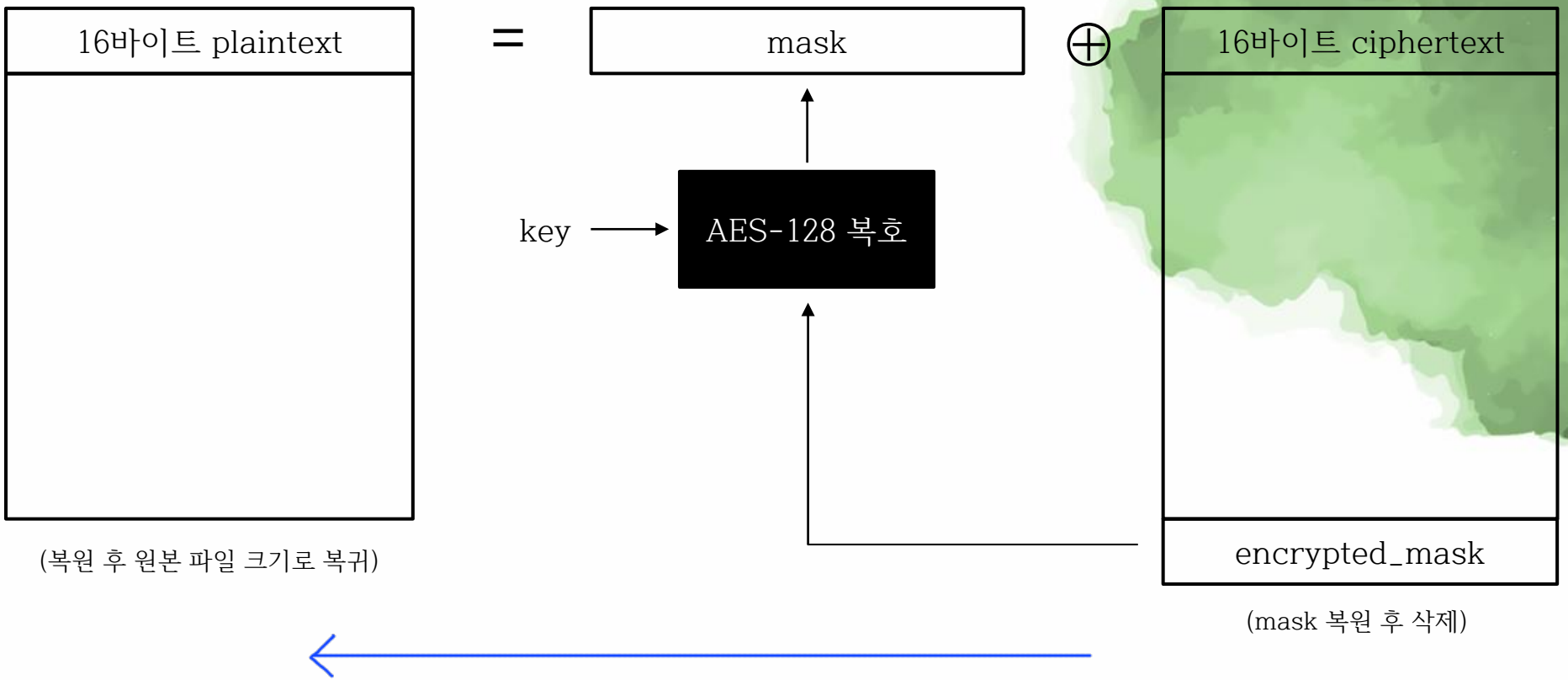
Assignment #2

./dkuware attack “key”



Assignment #2

./dkuware restore “key”



Assignment #2

Usage :

- 프로그램 인자의 수나 형식의 correctness를 체크하여 적절히 조치할 것
- 프로그램 2번째 인자로 스레드 함수 2개 (공격 / 복원, attack/restore) 중 택일
  - void * attack(void *param);
  - void * restore(void *param);
  - main 함수 안에 function pointer 변수 f를 선언할 것
  - 프로그램 실행 시 입력된 2번째 argument에 따라 attack 또는 restore 함수를 f에 매핑하여 pthread_create에 입력
- 프로그램 3번째 인자 (password) 로부터 16 바이트 추출하여 암/복호화 비밀키로 사용 (부족시 0 패팅)
- main thread는 pthread_join으로 2개의 child thread가 종료하기를 기다림
- 모든 대상 파일 공격/복원 완료 후에는 note 출력 (제공)

Assignment #2

- 프로젝트 구성
  - target (directory, 공격 대상 파일 위치)
  - dkuware.c
    - main 함수
    - 스레드 함수 등
  - crypto.c (+ crypto.h)
    - aes-128 암/복호 연산 등
  - utils.c (+ utils.h)
    - ransom note 출력 등
  - Makefile
- 헤더 파일은 header guard로 보호할 것
- 주석 정성껏 달 것

header 2번 이상 include 방지

Assignment #2

- OpenSSL 개발자 패키지 설치 → aes-128 암/복호
  - sudo apt-get install libssl-dev openssl
  - 첨부된 예제 파일 참고
- Makefile에 LDFLAGS 추가

```
CC = gcc                                    #컴파일러
TARGET = dkuware                            #프로그램명
OBJS = dkuware.o crypto.o utils.o           #오브젝트 파일들
CFLAGS= -Wall -g                            #컴파일 옵션
LDFLAGS = -pthread  -lcrypto   -lssl        #링커 옵션. 링크할 라이브러리들. -lpthread 등

all: $(TARGET)                              #최종 파일 명시

$(TARGET): $(OBJS)
    $(CC)  -o $@ $^ $(LDFLAGS)

.c.o:
    $(CC) $(CFLAGS) -c -o $@ $<

clean:
    rm -f $(OBJS) $(TARGET)
```

pthread flag 정보 삽입 시 L 빼 이유
: 라이브러리 링크 + 스레드 관련 컴파일 옵션 설정

Assignment #2

- 공격 전 target 디렉토리 내 샘플 파일

파일명 : jpg_sample1.jpg
크기 : 1,642,942 바이트

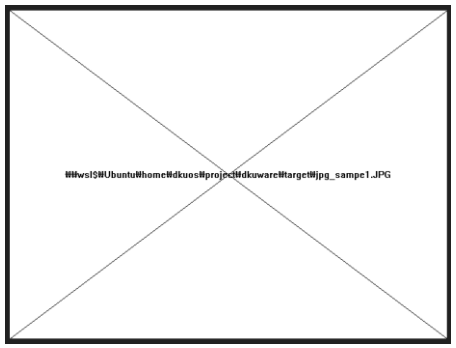
파일명 : jpg_sample2.jpg
크기 : 2,921,925 바이트

파일명 : pdf_sample1.pdf
크기 : 161,917 바이트

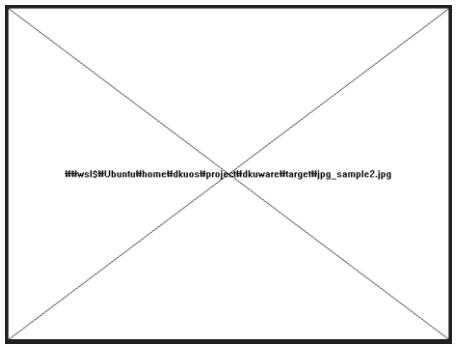
파일명 : pdf_sample2.pdf
크기 : 60,982 바이트

Assignment #2

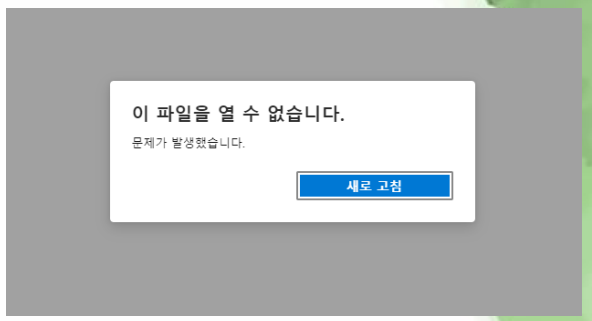
- 공격 수행 후 target directory 새로 고침 → 4개의 파일이 오픈 안됨



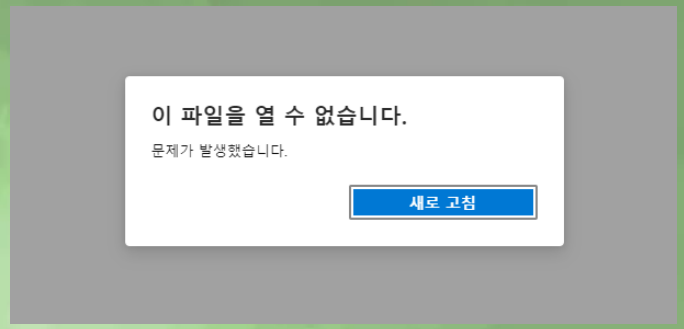
파일명 : jpg_sample1.jpg
크기 : 1,642,958 바이트



파일명 : jpg_sample2.jpg
크기 : 2,921,941 바이트



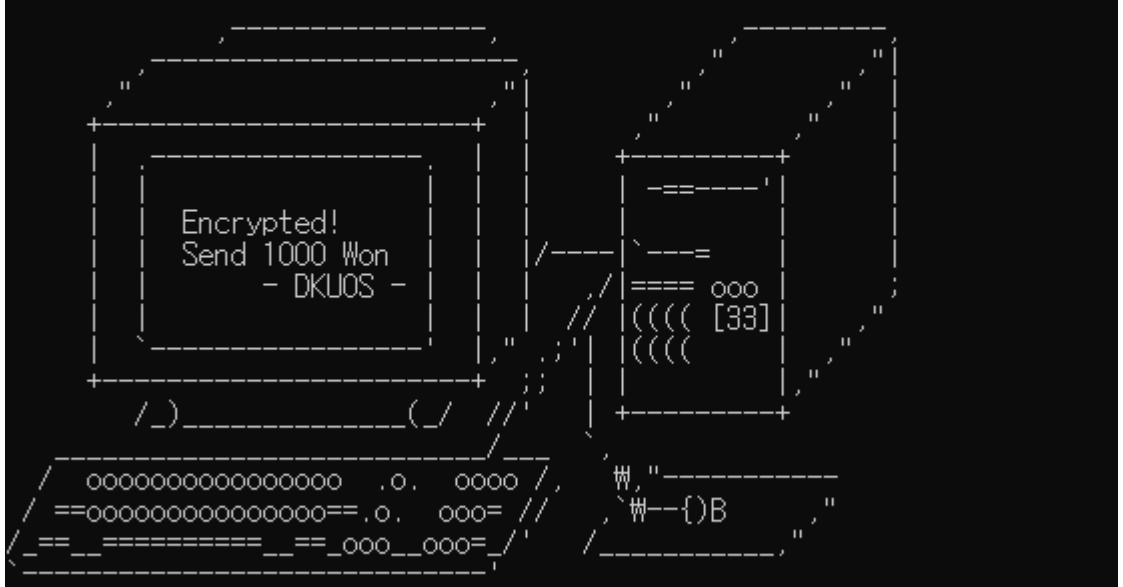
파일명 : pdf_sample1.pdf
크기 : 161,933 바이트



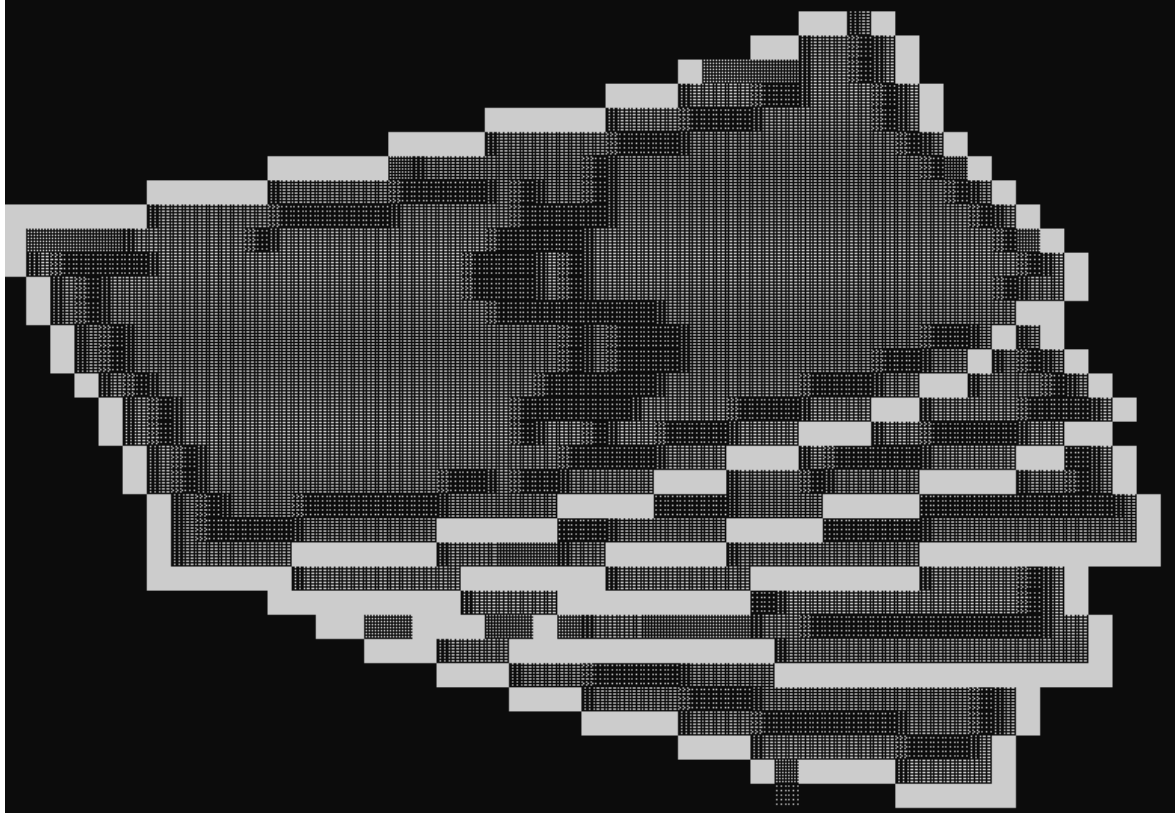
파일명 : pdf_sample2.pdf
크기 : 60,998 바이트

- 복원 수행 후 target directory 새로 고침 → 4개의 파일 원본 복구

```
dkuos@DB400TDA:~/project/dkuware$ ./dkuware attack "this is my key"
[attack] jpg_sample2.jpg
[attack] pdf_sample1.pdf
[attack] jpg_sampe1.JPG
[attack] pdf_sample2.pdf
[attack] 2 jpg files were encrypted
[attack] 2 pdf files were encrypted
```




```
dkuos@DB400TDA:~/project/dkuware$ ./dkuware restore "this is my key"
[restore] jpg_sample2.jpg
[restore] pdf_sample1.pdf
[restore] pdf_sample2.pdf
[restore] jpg_sampe1.JPG
[restore] 2 pdf files were decrypted
[restore] 2 jpg files were decrypted
```



```
Thank you very much~ from DKUOS!
```