aws 서버 종료 및 계정 종료

- **aws 서버가 구동 중인 상태에서 잊고 있으면 1년 후에 요금이 과금될 수 있음**
  - 서버를 반드시 종료할 것
  - 한달 후에 과금되는 내용이 없음을 확인할 것
- **aws 계정 해킹 사고가 많으니 계정을 폐쇄할 것(의무 아님)**
  - 계정을 해킹 당하면 많은 비용이 부과될 수 있음
  - 불의의 사고를 예방하기 위해 계정 폐쇄를 권고함

과제 4 방화벽/암호화 프로그램

AI융합전공

과제 4

- **제출 마감일 :**
  - 12월 3일 (일요일) 11:59pm 까지
- **eClass 과제방에 제출**
- **개인 과제**
- **개발 언어 : C/C++/Java/Python 외**
  - python 추천
- **제출 양식**
  - 문서 (PPT/PDF/HWP), 프로그램 소스코드

1. AES 암복호화 프로그램

- **사용자가 입력한 문장을 AES 암복호화를 진행한다. 다음의 2가지 기능이 지원된다.**
  - 사용자가 입력한 일반 문장을 암호화 하여 표시한다.
  - 사용자가 입력한 암호화 문장을 복호화 하여 표시한다.
- **AES를 지원하는 라이브러리 또는 패키지를 가져와 사용한다.**
  - 어느 라이브러리/패키지를 썼는지 명시한다.
- **Key는 개인이 정해서 사용한다.**
  - 그 Key가 무엇이고, 어떻게 정했는지 설명한다.
  - 프로그램 실행할 때 Key는 동일해야 한다. Key가 달라지면 암호화 결과가 달라진다.

1. AES 암복호화 프로그램

- **실행 예**

  1. 암호화
  2. 복호화

  메뉴를 선택하세요 *1*

  문장 : *goodmorning*

  암호화 : qtEUafvjxXqZ1HM=

  1. 암호화
  2. 복호화

  메뉴를 선택하세요 *2*

  문장 : *qtEUafvjxXqZ1HM=*

  복호화 : goodmorning

1. AES 암복호화 프로그램

- **주의할 점**
  - AES 암호화의 결과는 문자가 아니라 이진 데이터로 나온다.
    - 예) b'W₩x82₩x1b₩xea₩xf5₩x1fP₩xdd₩xba₩xbco'
  - 암호화된 문장이 이진데이터로 나오면 전달하기가 어렵다. 따라서 문자 형태로 바꾸어 사용하는 것이 좋다.(base64 참고)

2. 해시를 이용한 파일 변조 확인

- 대표적 해시 알고리즘인 MD5를 이용한다.
- 파일 이름을 입력하면 해당 파일의 내용을 분석하여 MD5 값을 표시한다. 파일을 먼저 다운로드 한 후, 그 파일의 내용을 분석하는 것이다.
- 예제 파일은 파이썬 다운로드 페이지의 파일들을 이용한다. 표시된 MD5와 우리 프로그램이 계산한 MD5가 일치하는지 확인한다.

Files

Version	Operating System	Description	MD5 Sum	File Size	GPG	Sigstore	
Gzipped source tarball	Source release		c5f77f1ea256dc5bdb0897eeb4d35bb0	26333656	SIG	CRT	SIG
XZ compressed source tarball	Source release		fe92acfa0db9b9f5044958edb451d463	19819768	SIG	CRT	SIG
macOS 64-bit universal2 installer	macOS	for macOS 10.9 and later	98fa94815780c9330fc2154559365834	42602603	SIG	CRT	SIG
Windows embeddable package (32-bit)	Windows		0888959642cc8af087d88da3866490a5	9560053	SIG	CRT	SIG
Windows embeddable package (64-bit)	Windows		7df0f4244e5a66760b7caaed58e86c93	10545380	SIG	CRT	SIG
Windows embeddable package (ARM64)	Windows		e3dbbd5d63c6cb203adc6c0c8ca5f5f7	9765886	SIG	CRT	SIG

2. 해시를 이용한 파일 변조 확인

- **실행 예**

미리 다운로드 한 후, 파일을 읽어 사용한다.

파일 이름을 넣으세요. *python-3.11.0-embed-win32.zip*

파일의 해시 값(md5)은 0888959642cc8af087d88da3866490a5

출력된 해시값과 사이트의 해시값이 일치한다. 즉 사이트의 파일과 내가 가진 파일은 동일하다.

Files

Version	Operating System	Description	MD5 Sum	File Size	GPG	Sigstore	
Gzipped source tarball	Source release		c5f77f1ea256dc5bdb0897eeb4d35bb0	26333656	SIG	CRT	SIG
XZ compressed source tarball	Source release		fe92acfa0db9b9f5044958edb451d463	19819768	SIG	CRT	SIG
macOS 64-bit universal2 installer	macOS	for macOS 10.9 and later	98fa94815780c9330fc2154559365834	42602603	SIG	CRT	SIG
Windows embeddable package (32-bit)	Windows		0888959642cc8af087d88da3866490a5	9560053	SIG	CRT	SIG
Windows embeddable package (64-bit)	Windows		7df0f4244e5a66760b7caaed58e86c93	10545380	SIG	CRT	SIG
Windows embeddable package (ARM64)	Windows		e3dbbd5d63c6cb203adc6c0c8ca5f5f7	9765886	SIG	CRT	SIG