컴퓨터보안 14주차

2023. 06. 07. (Wed)

Table of Contents

실습1 : 대칭키 암호/복호 AxCrypt 설치 및 사용

- **AxCrypt 소개 및 설명 1**
  - AxCrypt는 Windows 환경에서 널리 사용되는 공개용 파일 암호화 소프트웨어(file encryption software)로 파일들의 암호화, 복호화 그리고 저장 및 전송이 가능하도록 통합서비스를 제공한다. 200만명이 넘는 사용자를 자랑하니 프로그램의 안정성은 어느 정도 검증되었다고 볼 수 있다.
  - AxCrypt는 https://www.axcrypt.net/information/legacy-downloads/에서 Windows OS type별로 무료로 다운로드 받을 수 있다. 인스톨없이 사용가능한 버전은 기능이 제한되므로 반드시 정확한 설치를 통해서 사용해야 한다. 설치후 사용법은 각자 익힌다.
  - AxCrypt는 하나의 독립된 프로그램에 의해 작동하지 않고, 탐색기(Windows explorer)와 통합된 형태로 실행된다. 기본적으로 탐색기에서 파일이나 폴더를 우클릭함으로써 AxCrypt의 사용 메뉴를 불러올 수 있다. 특히, 암호화(encrypt)하기, 암화화된 파일 열기, 복호화(decrypt)하기 등등의 메뉴 사용법을 익힌다.

실습1 : 대칭키 암호/복호 AxCrypt 설치 및 사용

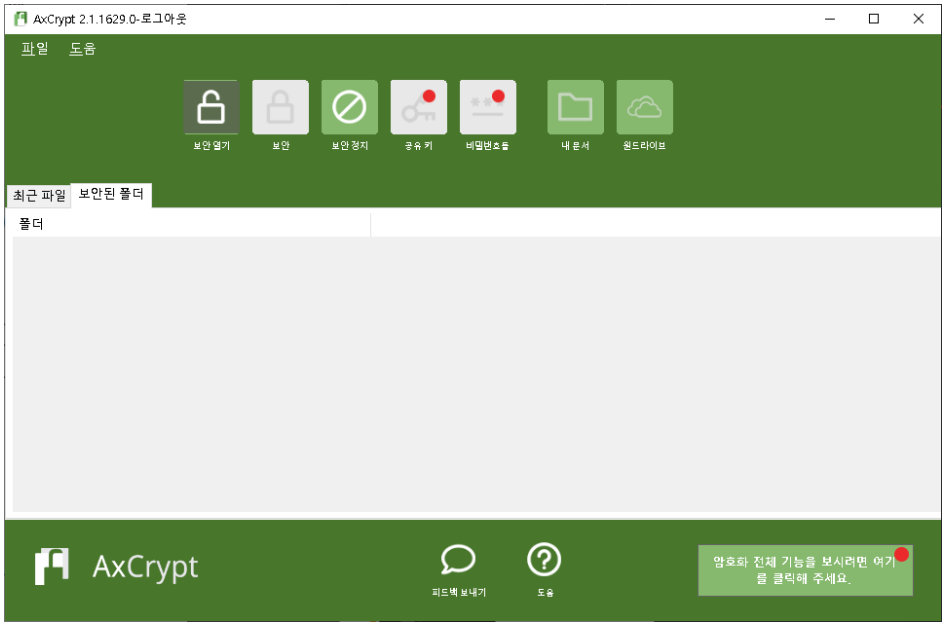
- **AxCrypt 소개 및 설명 2**
  - 일반적으로 [Encrypt]를 위한 메뉴에서 암호를 위해 passphrase를 사용하는 것 이외에 [Make Key-File]을 실행시켜 랜덤하게 생성된 'Key-File' 텍스트 문서를 이용하여 암호화할 경우, 대상파일을 AES-128 정도의 매우 강력한 암호로 보호할 수 있다.

  - 다른 암호화 메뉴로 [Encrypt] 이외에 원본파일을 유지한 채 추가적으로 암호화된 파일을 생성하는 기능인 [Encrypt a copy]와 AxCrypt가 설치되지 않은 컴퓨터의 사용자도 복호화가 가능하도록 Self-Decrypter 파일을 생성하는[Encrypt copy to .EXE]가 있다.

실습1 : 대칭키 암호/복호 AxCrypt 설치 및 사용

- [과제 내용]
  - 아래의 각 문제에 대한 수행 결과를 캡처하여 분석하고 설명하는 내용을 개인적인 견해와 함께 레포트에 모두 반영하여야 한다.

  - 암호화할 각기 다른 형식의 파일들을 임의로 3개 준비하여 files 폴더에 담는다. (원본파일들은 실습 전 따로 backup하여 보관하시오). 새로운 폴더인 keys 폴더를 하나 만들고, 원본 파일들을 우클릭하여 파일 개수만큼 Key-File을 생성하고 keys 폴더에 옮겨놓는다.



최신 버전의 AxCrypt UI(유료화, 실습사용 X)

실습1 : 대칭키 암호/복호 AxCrypt 설치 및 사용

- [과제 내용]

1) 하나의 Key-File을 자기 자신을 Key-File로 하여 [Encrypt]했을 경우 어떤 일이 발생하는지 설명하라.
2) 하나의 Key-File을 자기 자신을 Key-File로 하여 [Encrypt a copy]를 실행시켰을 경우는 1번과 어떻게 달라지는지 설명하라.
3) 각각의 파일을 [Encrypt a copy]를 이용하여 암호화된 사본파일을 만들고, 이들을 하나의 폴더(폴더명은 Test라 하자)에 따로 저장한 뒤, 그 폴더 전체에 [Rename]을 실행시켜라. 폴더를 열어 암호화된 파일들이 어떻게 변하였는지 설명하라.
4) 3번 문제에서 각각의 파일마다 암호화 passphrase나 Key-File이 다를 경우, 파일들을 어떻게 구분해 낼 수 있는지 설명하라.
5) keys 폴더를 zip 파일로 압축한 뒤 [Encrypt]를 실행시켜라. 어떤 일이 발생하는가 ? 5번 문제와 비교하여 설명하라.
6) 우리는 Key-File을 생성해서 파일을 암호화할 경우 AES-128의 강도로 암호화할 수 있다는 것을 알았다. 하지만 파일들을 암호화할 때 항상 같은 Key-File을 사용하는 것이 아니라면, 위의 문제들과 같이 여러개의 Key-File이 생성하게 되고, 이것들을 관리하는 것 또한 보안유지를 위해 중요한 일이 된다. 그러면 5번과 6번 문제를 종합하여 Key-File의 효율적인 관리방안을 모색해 보아라.

실습2 : 공개키 암호/복호 GPG4Win 설치 및 사용

- **GnuPG 소개 및 설명 1**
  - GnuPG (GNU Privacy Guard)는 GNU 재단에서 개발한 이메일 및 파일 내용의 암호화와 복호화 기능을 제공하는 대표적인 프로그램이다. GPG4Win은 GnuPG의 윈도우 버전이라 할 수 있다. 본 과제에서는 GPG4Win을 활용하여 사용자가 작성한 평문을 암호화한 후, 암호화된 글을 다시 평문으로 복호화하는 과정에 대해 공부한다.

  - GPG4Win은 공식 홈페이지 (http://www.gpg4win.org)에서 무료로 다운로드할 수 있다. 설치시 [4단계]의 구성요소 선택에서는 Claws-Mail을 제외한 나머지 부분의 체크박스는 모두 선택하고, [8단계]의 설치시 주의사항이 팝업 창으로 나타날 경우, 관련내용을 확인한 후 확인버튼을 선택하여 나머지 설치를 완료한다. 자세한 사용법은 홈페이지에서 제공하고 있는 사용자 가이드를 PDF버전으로 다운받아 참조할 수 있다.

  - GPG4Win 프로그램에서 1) GPA를 이용하여 비밀키와 공개키 생성하기, 2) 공개키 추출 및 공유하기, 3) 상대의 공개키 등록 및 암호문 작성, 4) 암호문 전달 및 복호화 과정, 5) 전자서명, 6) 암호화 및 전자서명을 동시에 하기, 7) 공개키를 교환하는 방식 등등을 자세히 익힌다.

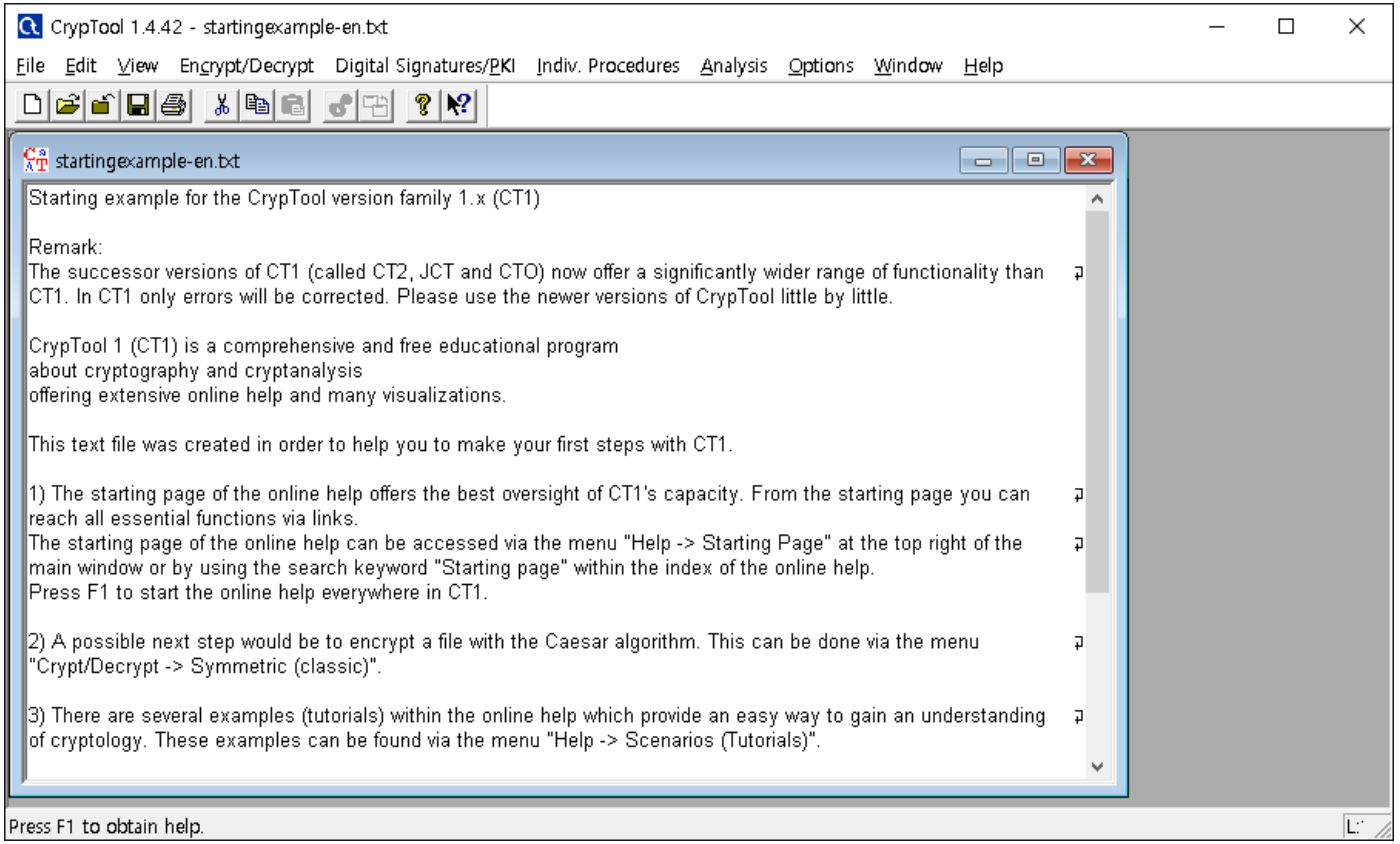
실습2 : 공개키 암호/복호 GPG4Win 설치 및 사용

- [과제 내용]
  - 아래의 각 문제에 대한 수행 결과를 캡처하여 분석하고 설명하는 내용을 개인적인 견해와 함께 레포트에 모두 반영하여야 한다. (1 ~ 3번은 GPA 이용)
    1) GPA(Kleopatra)를 이용하여 Alice와 Bob의 비밀키와 공개키를 생성하고 과정과 결과를 설명하라.
    2) 2명 모두 공개키 추출을 진행하고 공개키를 서로 공유하는 시나리오를 생각해보고 작성하라.
    3) 본인이 상상한 시나리오를 기반으로 각각 상대의 공개키 등록 및 암호문을 작성해 보아라.
    4) 암호문 전달 및 복호화 과정을 본인이 생각한 시나리오를 바탕으로 설명하라
    5) 여기서 전자서명은 무엇인가? 어떻게 이용될 수 있는가? 적합할 수 있는가?
    6) 암호화 및 전자서명을 동시에 사용하는 방법을 설명하라.
    7) 공개키를 교환하는 방식에 대해 본인이 작성한 시나리오를 그림으로 작성하라.

실습3 : CrypTool

- **CrypTool**
  - 이번 실습은 크래킹 횟수와 키 길이의 연관성을 보여준다. 실습을 위하여 https://www.cryptool.org/en/ct1/ 에서 다운로드 한다.

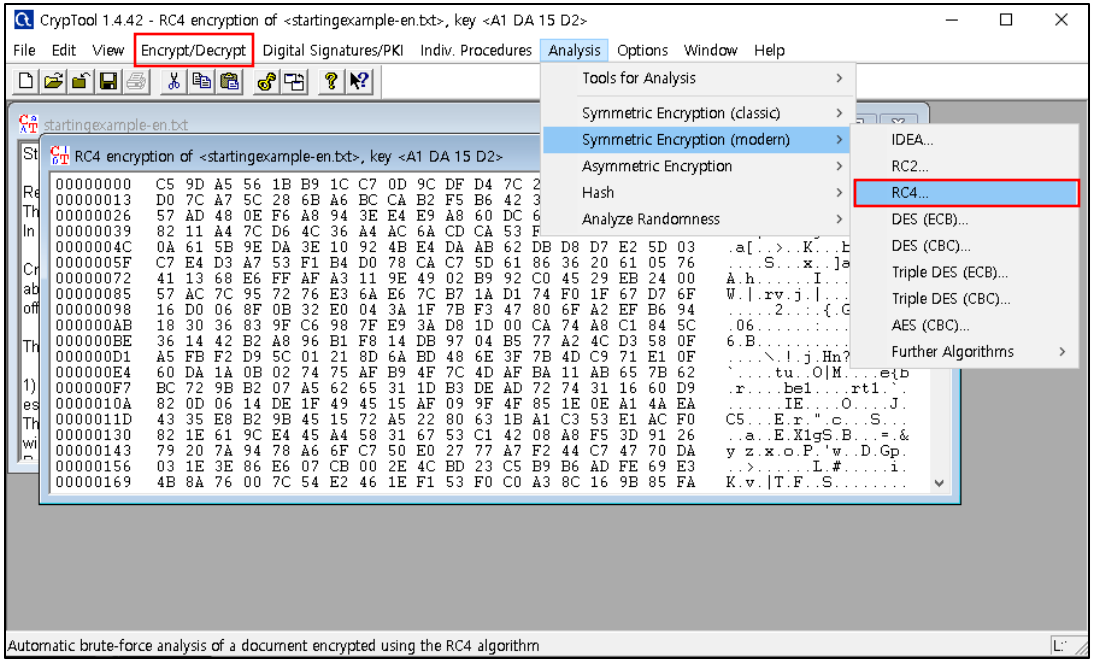
1) CrypTool을 설치하고 모든 기본 세팅을 설정한다. 설치가 되면 프로그램은 아래 그림과 같이 보인다.



실습3 : CrypTool

2) 메뉴에서 Enrypt/Decrypt > Symmetric (Modern) > RC4를 선택한다. 8비트 키 길이를 입력하고 Encrypt를 선택한다.

3) 아래의 첫번째 그림에 보이는 것처럼 Analysis > Symmetric Encryption (modern) > RC4를 선택한다. 8비트 키를 선택하고 Brute-Force Decrypt를 시작한다. 얼마나 빠르게 평문이 나타나는지 확인한다.



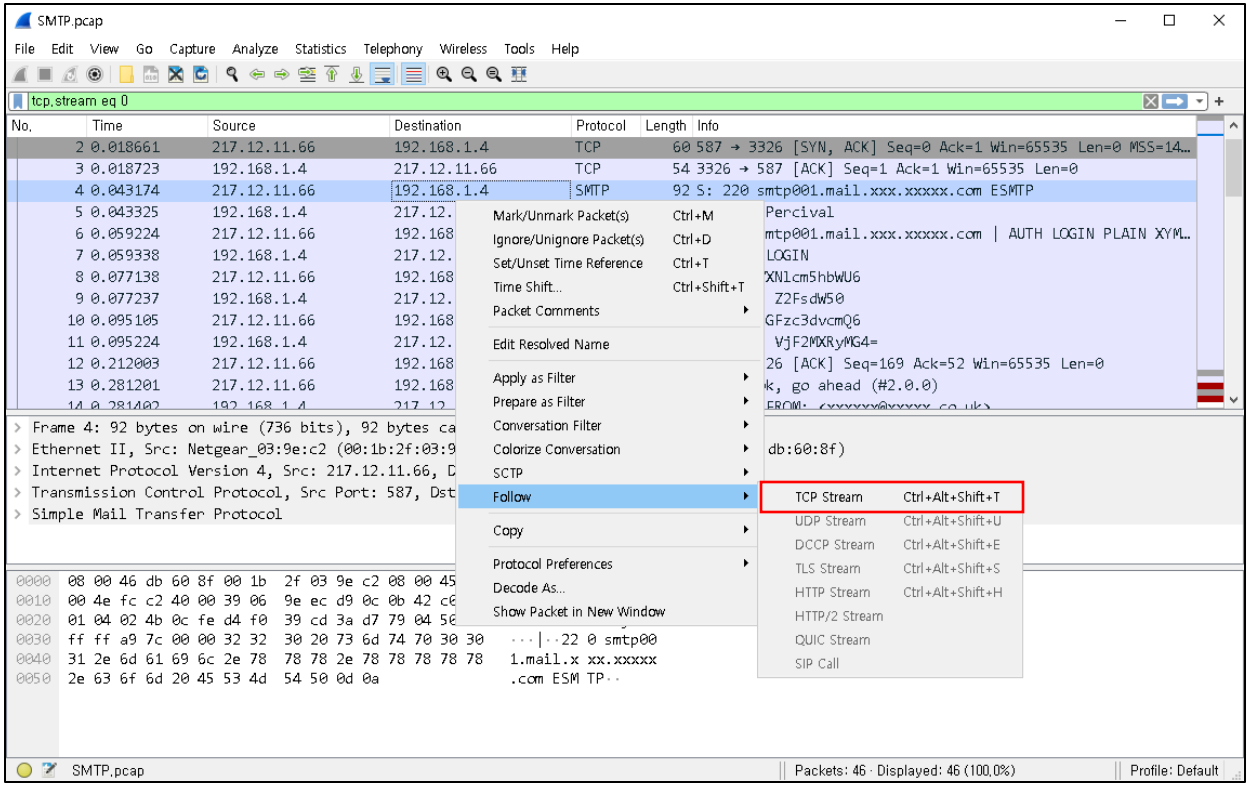
4) 16비트 키, 32비트 키를 입력해서 2단계와 3단계를 반복해본다. 아래의 두번째 그림처럼, 32비트 키는 복호화하는데 상당히 더 오래 걸림을 알 수 있다.

실습4 : 이메일 사용자 이름과 패스워드 추출

- **Wireshark 실습**
  - 이번 실습에서는 SMTP.pcap 파일을 통해 SMTP 캡처에서 사용한 이름과 패스워드를 추출할 것이다.

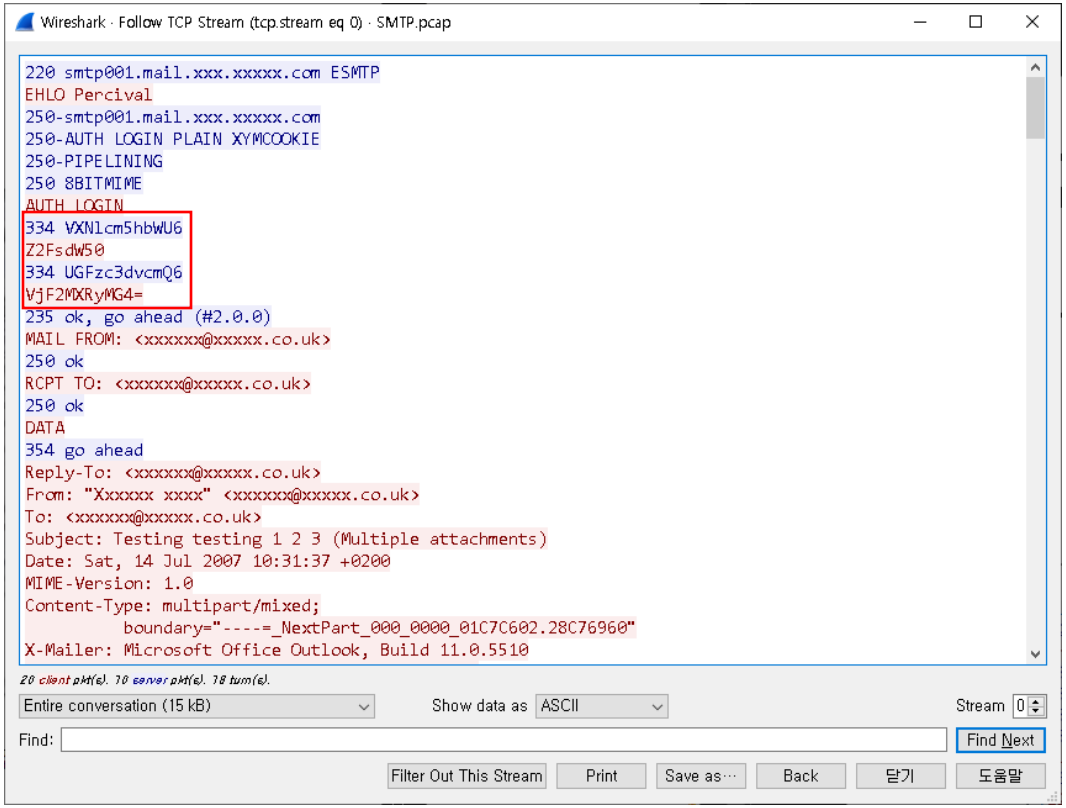
    1) 와이어샤크를 실행하고 SMTP.pcap 파일을 연다.

    2) 아무 패킷에서 우클릭 후, 아래 그림처럼 Follow TCP Stream을 선택한다.



실습4 : 이메일 사용자 이름과 패스워드 추출

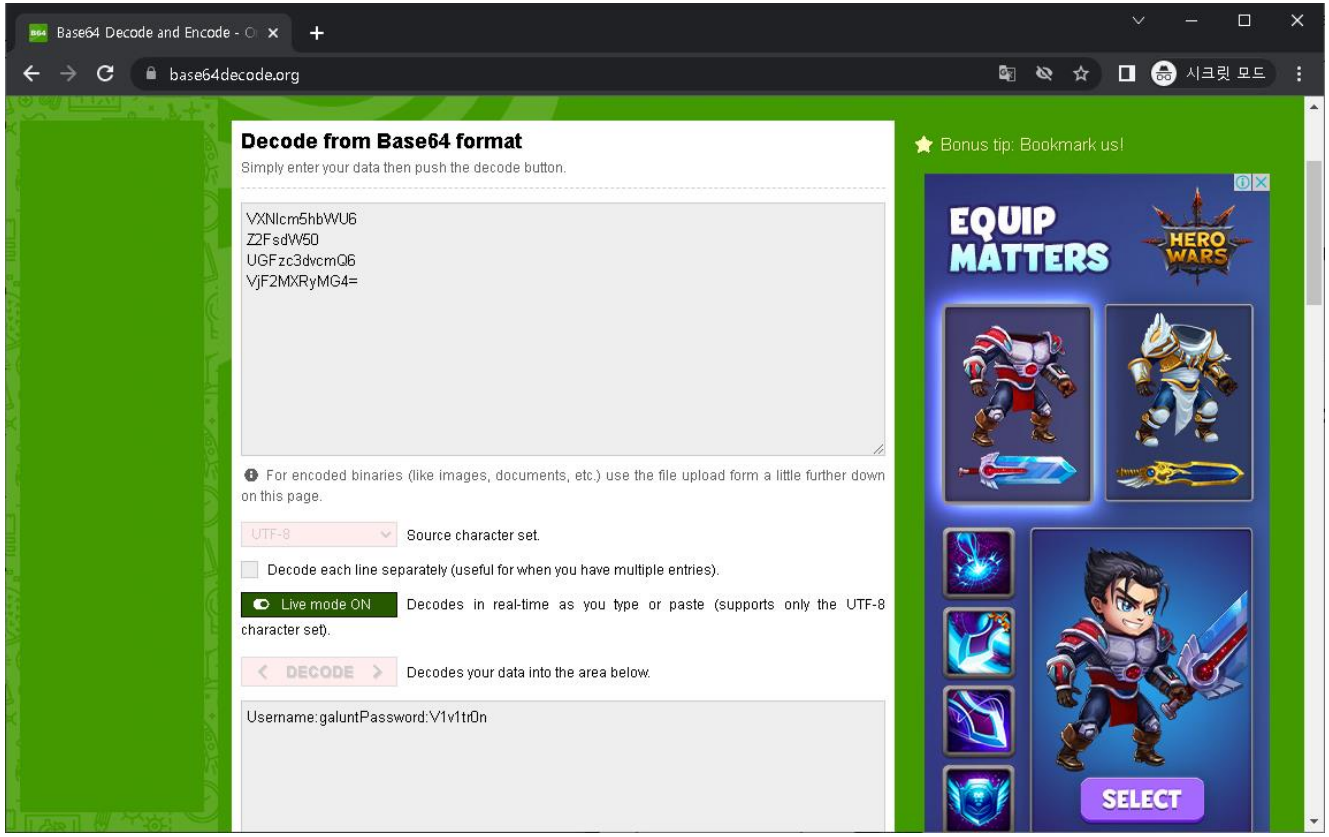
3) 스트림을 관찰하고, 다음의 그림처럼 334 값을 찾는다. 이것은 Base64로 인코딩된 평문 사용자 이름과 패스워드 문자열이다.



4) 브라우저를 열어 https://www.base64decode.org/ 를 방문한다. 이것은 Base64 디코더이다.

실습4 : 이메일 사용자 이름과 패스워드 추출

5) 각 값을 입력하고 결과를 살펴본다. 사용자 이름은 galunt, 패스워드는 V1v1tr0n 으로 보일 것이다. 패스워드는 아래 그림에서 보는 바와 같다.



이 실습은 강력한 암호를 사용하지 않고 이메일 서비스를 이용하는 것에 대하여 생각하도록 만들 것이다.

컴퓨터보안 14주차

QNA