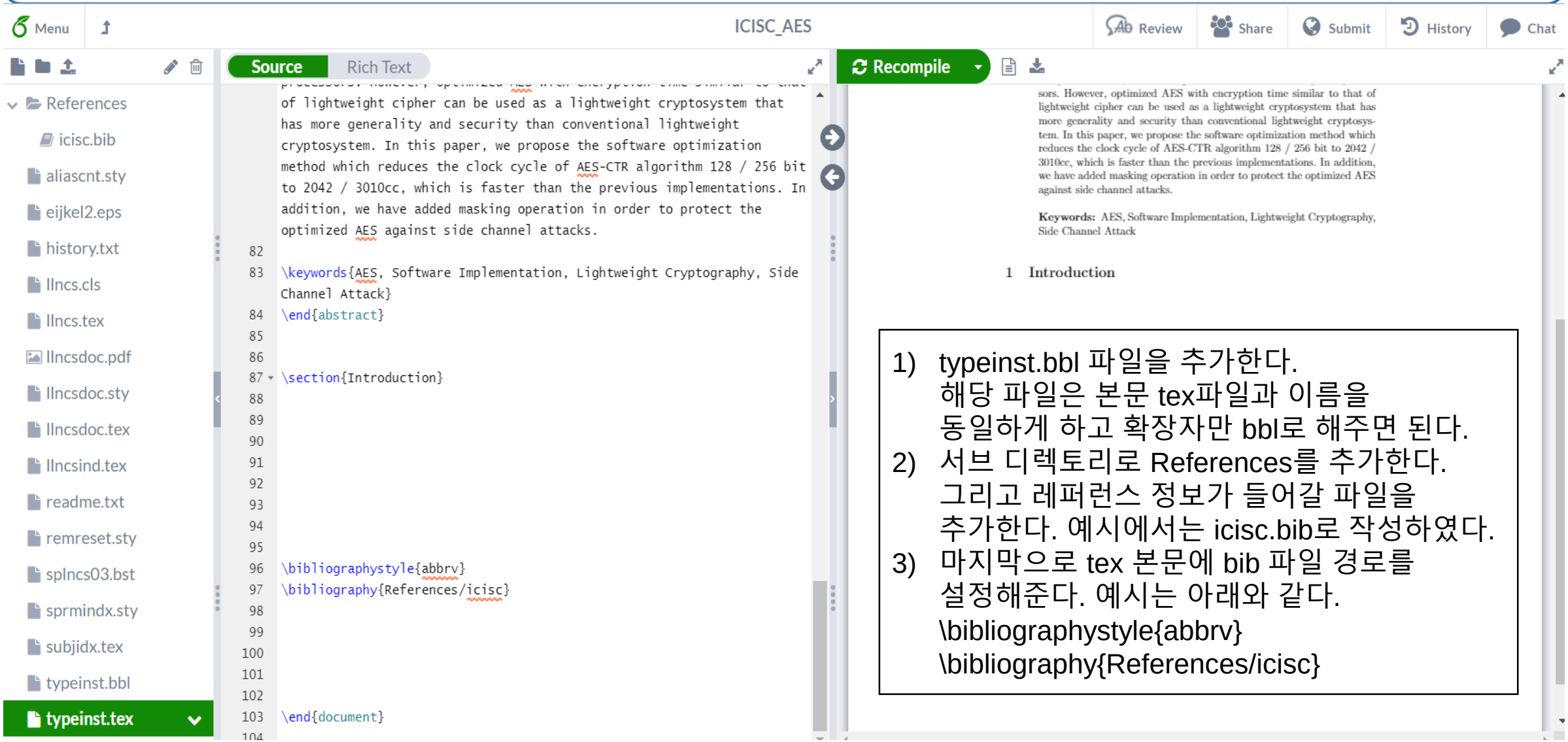
LaTex 레퍼런스 추가

한성대학교 서화정

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

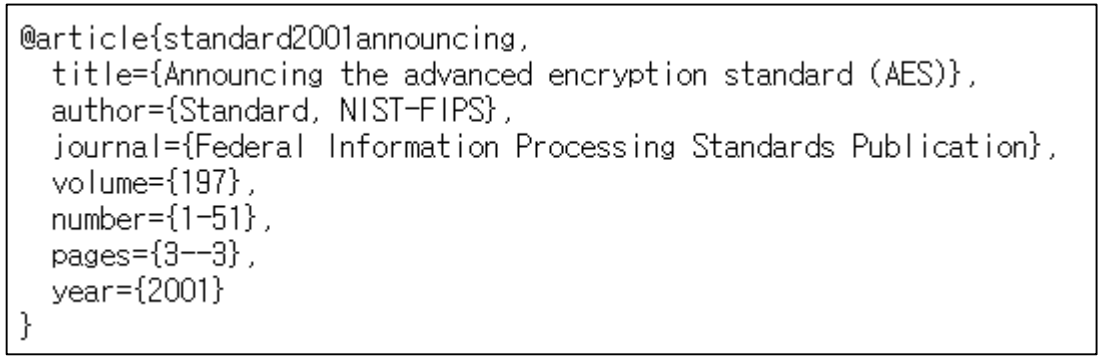
LaTex 레퍼런스 추가 설정



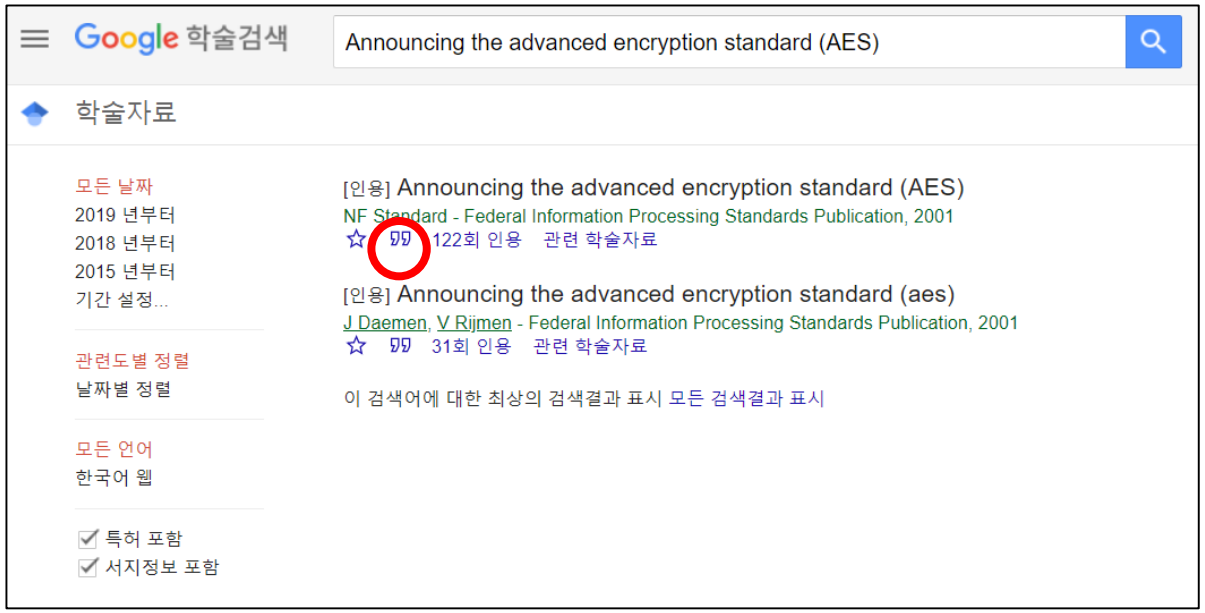
1) typeinst.bbl 파일을 추가한다.
   해당 파일은 본문 tex파일과 이름을 동일하게 하고 확장자만 bbl로 해주면 된다.
2) 서브 디렉토리로 References를 추가한다.
   그리고 레퍼런스 정보가 들어갈 파일을 추가한다. 예시에서는 icisc.bib로 작성하였다.
3) 마지막으로 tex 본문에 bib 파일 경로를 설정해준다. 예시는 아래와 같다.
   \bibliographystyle{abbrv}
   \bibliography{References/icisc}

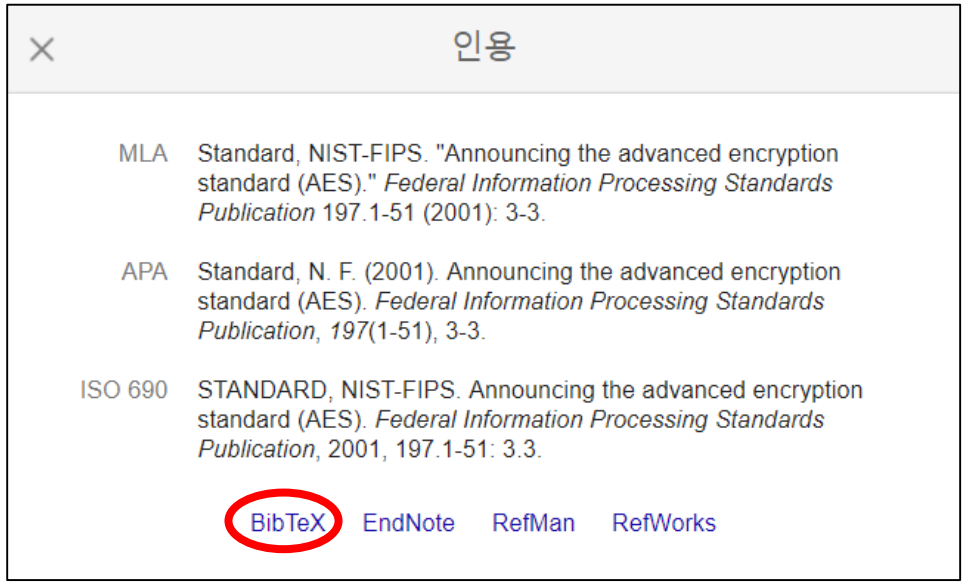
LaTex 레퍼런스 추가

명시된 순서대로 논문을 검색 후 최종적으로 논문에 대한 정보를 확보하게 된다.



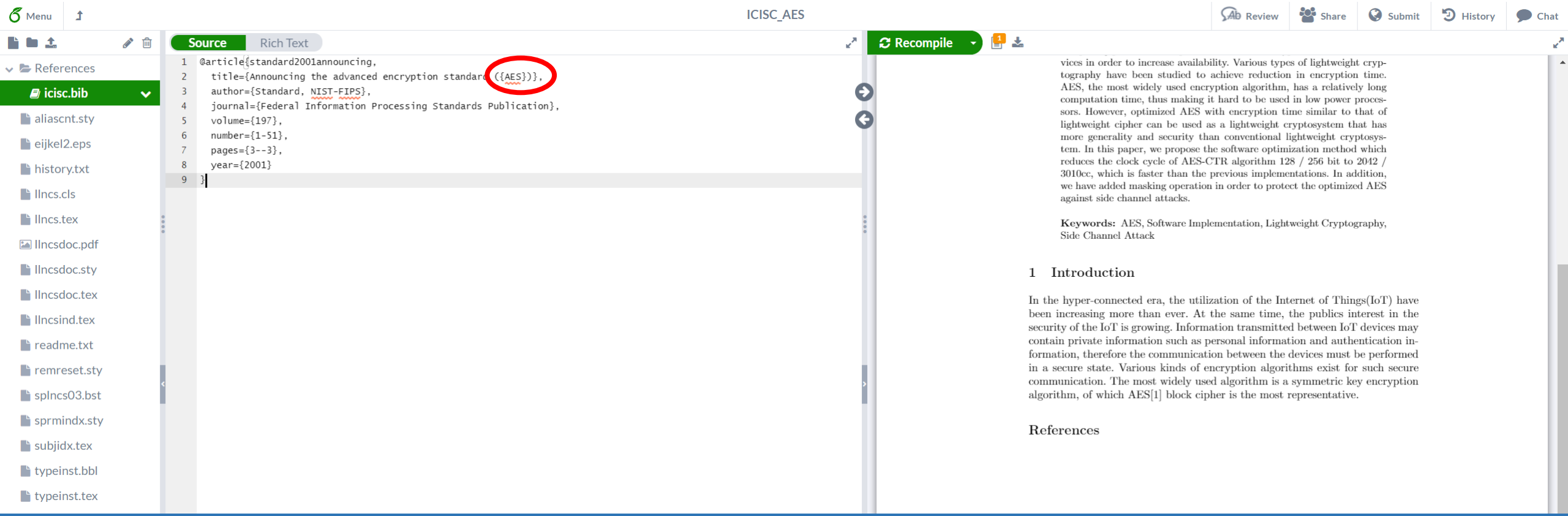
```
@article{standard2001announcing,
  title={Announcing the advanced encryption standard (AES)},
  author={Standard, NIST-FIPS},
  journal={Federal Information Processing Standards Publication},
  volume={197},
  number={1-51},
  pages={3--3},
  year={2001}
}
```





LaTex 레퍼런스 추가

- 해당 정보를 긁어서 bib 파일에 추가한다.
- AES와 같은 대문자로 나타나야 하는 문구에는 중괄호 "{", "}" 를 이용하여 묶어 주어야 대문자로 표기된다.



LaTex 레퍼런스 추가

- \cite 명령어로 해당 레퍼런스의 이름을 적어준다.

```
\section{Introduction}
In the hyper-connected era, the utilization of the Internet of Things(IoT) have been increasing more than ever. At
the same time, the public's interest in the security of the IoT is growing.
Information transmitted between IoT devices may contain private information such as personal information and
authentication information, therefore the communication between the devices must be performed in a secure state.
Various kinds of encryption algorithms exist for such secure communication. The most widely used algorithm is a
symmetric key encryption algorithm, of which AES \cite{standard2001announcing} block cipher is the most
representative.
```

LaTex 레퍼런스 추가

- 컴파일을 수행 하면 해당 레퍼런스가 추가된다.

1 Introduction

In the hyper-connected era, the utilization of the Internet of Things(IoT) have been increasing more than ever. At the same time, the publics interest in the security of the IoT is growing. Information transmitted between IoT devices may contain private information such as personal information and authentication information, therefore the communication between the devices must be performed in a secure state. Various kinds of encryption algorithms exist for such secure communication. The most widely used algorithm is a symmetric key encryption algorithm, of which AES [1] block cipher is the most representative.

References

1. N.-F. Standard. Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, 197(1-51):3–3, 2001.