독서클럽 모임 보고서 - 암호, 비밀을 지키는 과학

<table>
<tr><td rowspan="8">1주차</td><td>일시</td><td colspan="2">4월 8일 18:00~18:30 학술정보관 3F 그룹스터디실</td></tr>
<tr><td rowspan="6">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>김서정 (2353039)</td><td>O</td></tr>
<tr><td>조가희 (2694026)</td><td>O</td></tr>
<tr><td>김희은 (2553052)</td><td>O</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>진도</td><td>도서명: 암호, 비밀을 지키는 과학</td><td>진도페이지: 1p. ~ 60p.</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 조가희, 김희은, 김서정]

첫 모임에선 각자의 소개와 책에 대한 설명을 들었습니다. 암호, 비밀을 지키는 과학은 과거 고전 암호부터 현대의 컴퓨터 기술이 발명되고 나서의 암호까지 시대별로 설명되어 있습니다. 1P~60P는 고전 암호에 대해서 설명하고 있어 읽고 암호란 어떤 것인지 암호의 정의와 시작점에 대해 공부했습니다.</td></tr>
</table>

<table>
<tr><td rowspan="8">2주차</td><td>일시</td><td colspan="2">5월 29일 09 : 30 ~ 10: 10 학술정보관 3F 그룹스터디실</td></tr>
<tr><td rowspan="6">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>김서정 (2353039)</td><td>O</td></tr>
<tr><td>조가희 (2694026)</td><td>O</td></tr>
<tr><td>김희은 (2553052)</td><td>O</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>진도</td><td>도서명: 암호, 비밀을 지키는 과학</td><td>진도페이지: 60p. ~ 94p.</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 조가희, 김희은, 김서정]

두 번째 모임인 이번 진도에는 저번에 읽었던 고전 암호보다 조금 더 현대에 가까워진 암호 방식에 대해 읽었습니다. DES를 쉽게 풀지 못하게 만든 것이 AES인데 이 암호는 현대에도 쓰일 정도로 푸는 것이 어렵고 슈퍼 컴퓨터로 푼다고 해도 최소 1억년이 걸린다고 합니다. 조가희님은 관련 내용을 수업에서 배운다고 하셨습니다. 김희은님은 어렵지만 흥미로운 얘기가 많아 즐겁다고 하셨습니다. 저는 1900년대에 만들어진 암호가 기술이 많이 발전한 현대에까지 풀지 못하고 계속 쓰인다는 점이 신기했습니다. 마지막 챕터에 나오는 양자 암호에 대응하기 위한 양자 컴퓨터가 나오면 AES를 푸는 시간이 1년에서 6개월로 대폭 단축된다고 합니다. 암호를 빨리 푸는 만큼 개인정보가 위험해지지 않을까, AI의 발전에 어떻게 살아가야 할까 고민해보는 시간이었습니다.</td></tr>
</table>

<table>
<tr><td rowspan="8">3주차</td><td>일시</td><td colspan="2">5월 13일 18 : 00 ~ 18:40 학술정보관 5F 그룹스터디실</td></tr>
<tr><td rowspan="6">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>김서정 (2353039)</td><td>O</td></tr>
<tr><td>조가희 (2694026)</td><td>O</td></tr>
<tr><td>김희은 (2553052)</td><td>O</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>진도</td><td>도서명: 암호, 비밀을 지키는 과학</td><td>진도페이지: 95p. ~ 131p.</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 김서정, 조가희, 김희은]

3장은 2장의 키 교환 문제를 해결해주는 방법에 대한 얘기였습니다. 디피-헬먼 키 교환은 물감섞기로 비유합니다. 모두가 아는 색에 각자 비밀의 색을 섞으면 완성된 색은 비밀의 색을 넣은 당사자들만 아는 것입니다. 섞인 물감은 다시 원래의 색으로 돌리기 힘들다는 점처럼 디피-헬먼 키 교환 또한 일방향 함수를 이용해 계산은 쉽지만 다시 복호화가 어렵습니다. 해시라는 것도 이용하는데 이것은 암호를 보낸 사람이 정말 그 사람이 맞는지 증명해주는 것입니다. 현재 많은 사이트나 전자메일, 비밀번호에도 사용하고 있는 것으로 암호를 해시문으로 변환해 저장하기 때문에 해킹당해도 암호의 원문이 아닌 해시문이 나와 안전에 강하다는 점이 특징입니다. 일상에서 우리가 알지 못하는 곳에서도 많은 암호의 보호를 받고 있다는 점을 깨달은 시간이었습니다.</td></tr>
</table>

<table>
<tr><td rowspan="8">4주차</td><td>일시</td><td colspan="2">5월 27일 18 : 00 ~ 18:40 상상관 12층 한담</td></tr>
<tr><td rowspan="5">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>김서정 (2353039)</td><td>O</td></tr>
<tr><td>조가희 (2694026)</td><td>O</td></tr>
<tr><td>김희은 (2553052)</td><td>O</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>진도</td><td>도서명: 암호, 비밀을 지키는 과학</td><td>진도페이지: 132p. ~ 156p.</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 김희은, 조가희, 김서정

4장에서는 지금까지 나온 암호들을 조합해서 사용하는 프로토콜에 대해 설명해줍니다. 이를 위해서 인터넷이 나옵니다. 처음의 인터넷은 아주 좁고 취약한 연결을 갖고 있었습니다. 점점 규모가 커지자 보안이 필요해졌고 인증기관을 통해 응답을 주고받을 수 있게 되었습니다. 마지막 모임엔 서로 그동안의 활동 소감을 나누는 시간을 가졌습니다.</td></tr>
</table>

	No.	클럽원 정보	후기 내용
활동 후기	1	김서정 (2353039)	보안과 암호에 대해 막연히 비밀번호나 잠금장치만 알고 있었는데 책을 읽으며 살아가는데 사소한 부분도 암호의 도움을 받고 있었다는 걸 알게 됐다. 만약 암호가 없었다면 개인정보가 중요한 시대에 큰 위험이 있었을 것이다. 발명하는 사람도, 암호를 풀어내는 사람들 모두 대단하다고 생각이 들었다.
	2	조가희 (2694026)	『암호, 비밀을 지키는 과학』을 읽으며 독서 클럽 활동에 참여하였습니다. 책을 통해 암호가 단순히 비밀을 숨기는 기술이 아니라 정보 보안의 핵심 요소라는 점을 알 수 있었습니다. 또한 교수님과 선배님들의 설명을 들으며 혼자 읽을 때보다 내용을 더 쉽게 이해할 수 있었습니다. 특히 고전 암호가 현대 암호 기술로 발전해 온 과정이 인상 깊었으며, 암호학이 우리의 일상생활과 밀접하게 관련되어 있다는 점을 새롭게 느낄 수 있었습니다. 이번 활동을 통해 암호학에 대한 관심이 더욱 커졌습니다.
	3	김희은 (2553052)	평소에 접하기 어렵지만 관심은 있었던 보안에 대해 얕게나마 알 수 있어서 즐거웠다. 여태까지 해 온 독서클럽에서는 교수님께서 매 회차 참여하신 적이 없으셨는데, 이번 기수에서는 매번 와주시고 설명 해 주셔서 내용을 더 알차게 얻어 갈 수 있었다. 4번뿐인 짧은 만남이었지만 좋은 기억으로 남을 것 같다.
	4		
	5		