독서클럽 모임 보고서 - 크.마.(Cryptography Master)

<table>
<tr><td rowspan="7">1주차</td><td>일시</td><td colspan="2">4월 9일 17 : 00 공학관 A동 코딩라운지</td></tr>
<tr><td rowspan="5">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>형유림(2394016)</td><td>O</td></tr>
<tr><td>김하경(2394010)</td><td>O</td></tr>
<tr><td>손채민(2394032)</td><td>O</td></tr>
<tr><td>조수빈(2394025)</td><td>O</td></tr>
<tr><td>진도</td><td>도서명: 리얼월드 암호학</td><td>진도페이지: p.69 ~ p.93</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 석병진 교수님, 형유림, 김하경, 손채민, 조수빈]
김하경:
리얼월드 암호학의 챕터 4 [인증 암호화]에 대한 발표를 듣고 ECB와 CBC 모드의 차이점을 명확히 이해할 수 있었습니다. 특히 IV의 중요성에 대해 궁금증이 생겨 질문도 하며 토론에 참여했습니다.

손채민:
AES의 구조와 작동 방식(S-box, 라운드 키, SubBytes 등)에 대해 발표했고, 고정된 블록 크기와 키 길이로 인해 발생할 수 있는 한계점과 보안성 유지 조건에 대해 토론했다.

조수빈:
인증 암호화, 그 중에서도 AES를 중점적으로 발표하였다. 책 내에서 서술하고 있는 AES의 현재 활용 방안보다는 암호의 구현 과정에 대해서 집중적으로 발표를 진행하였으며, 부가적으로 운영 모드와 AES암호화에 인증을 적용하는 '연관 데이터 인증 암호화'에 대해서도 부가적으로 설명하였다.

형유림:
패딩 기술에 대해 질문하였으며 8바이트짜리 평문에 8바이트를 추가하는 예시로 PKCS#7표준 패딩의 개념을 답변으로 얻었다.</td></tr>
</table>

<table>
<tr><td rowspan="7">2주차</td><td>일시</td><td colspan="2">5월 20일 17 : 00 공학관 A동 상상파크 플러스</td></tr>
<tr><td rowspan="5">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>형유림(2394016)</td><td>O</td></tr>
<tr><td>김하경(2394010)</td><td>O</td></tr>
<tr><td>손채민(2394032)</td><td>O</td></tr>
<tr><td>조수빈(2394025)</td><td>O</td></tr>
<tr><td>진도</td><td>도서명: 리얼월드 암호학</td><td>진도페이지: p.269 ~ p.296</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 

[좌측부터 형유림, 손채민, 김하경, 손채민]

김하경:
리얼월드 암호학의 챕터 12 [‘암호화폐’의 ‘암호‘?]에 대한 발표를 들었습니다. 탈중앙화 시스템의 구조와 중앙화 시스템과의 비교에 흥미를 느꼈고, 비트코인의 트랜잭션 구조에 대해 질문을 했습니다.

손채민:
내가 발표를 맡은 주차로, 블록체인의 구조와 비트코인의 작동 원리를 소개했다. 이후 암호화폐의 익명성 문제와 범죄 악용 가능성, 추적 기술의 한계에 대해 다양한 의견을 나눴다.

조수빈:
지금은 현실적으로 비트코인 클러스터링 기법이 불가능하다고 하였지만, AI 및 컴퓨터의 연산 속도가 발전한다면 오프 체인 데이터를 이용하여 비트코인 클러스터링 기법이 실제로 가능할 것이라고 주장하였다.

형유림:
클리스터링 기법에서 복합 입력 주소 문제에 대한 해결 여부를 질문하였으며, 이론상으로는 가능하지만 현실적으로 조합 매칭은 매우 어렵다는 답변들 받았다.</td></tr>
</table>

<table>
<tr><td rowspan="7">3주차</td><td>일시</td><td colspan="2">5월 21일 17 : 00 지도교수님 연구실</td></tr>
<tr><td rowspan="5">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>형유림(2394016)</td><td>O</td></tr>
<tr><td>김하경(2394010)</td><td>O</td></tr>
<tr><td>손채민(2394032)</td><td>O</td></tr>
<tr><td>조수빈(2394025)</td><td>O</td></tr>
<tr><td>진도</td><td>도서명: 리얼월드 암호학</td><td>진도페이지: p.319 ~ p.343</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 형유림, 조수빈, 손채민, 김하경, 석병진 교수님]

김하경:
리얼월드 암호학의 챕터 14 [양자 컴퓨터 시대의 암호학]에 대한 발표를 했습니다. 양자 컴퓨터의 정의와 역사, 핵심 특성 2가지, 양자 내성 암호에 대해서 설명했습니다. 특히 핵심 특성 2가지인 양자 중첩과 양자 얽힘에 대해 팀원들이 이해할 수 있도록 집중적으로 설명했습니다.

손채민:
양자컴퓨터의 등장으로 기존 공개키 암호가 무력화될 수 있다는 문제 제기와 함께, 양자 내성 암호의 종류와 적용 가능성에 대해 토론했다.

조수빈:
컴퓨터로는 0또는 1 중 하나로만 표현할 수 있다고 생각했는데, 어떤 식으로 0과 1을 한 번에 계산할 수 있는 것인지, 이것이 실제 구현 가능한지 질문하였고, 초전도체를 절대 온도에 가깝게 냉각해 전기가 저항 없이 흐를 수 있도록 하여 0과 1의 중첩 상태를 가진 큐비트를 만들어낼 수 있다는 답변을 얻었다.

형유림:
PQC와 양자 내성 암호의 차이에 대해 질문하였고, PQC는 Post Quantum Cryptography, 즉 양자 후 암호이고 양자컴퓨팅 환경에 내성을 가지는 암호인 양자 내성 암호는 아직까지 난제라는 답변을 얻었다.</td></tr>
</table>

<table>
<tr><td rowspan="7">4주차</td><td>일시</td><td colspan="2">5월 30일 17 : 00 지도교수님 연구실</td></tr>
<tr><td rowspan="5">참여 학생</td><td>클럽원 정보</td><td>참석 여부</td></tr>
<tr><td>형유림(2394016)</td><td>O</td></tr>
<tr><td>김하경(2394010)</td><td>O</td></tr>
<tr><td>손채민(2394032)</td><td>O</td></tr>
<tr><td>조수빈(2394025)</td><td>O</td></tr>
<tr><td>진도</td><td>도서명: 리얼월드 암호학</td><td>진도페이지: p.297 ~ p.318</td></tr>
<tr><td>토론 내용</td><td colspan="2"> 
[좌측부터 형유림, 손채민, 조수빈, 김하경, 석병진 교수님]

김하경:
리얼월드 암호학의 챕터 13 [하드웨어 암호학]에 대한 발표를 듣고 사이드채널 공격에 대한 설명은 특히 흥미로웠습니다. 단순히 데이터를 훔치는 게 아니라 전력 소비나 소리, 타이밍 차이 같은 예상치 못한 요소를 통해 정보가 유출될 수 있다는 점에서, 보안이 얼마나 다층적이어야 하는지를 새삼 느꼈습니다.

손채민:
TPM, HSM 등의 하드웨어 보안 장치를 중심으로 발표가 이루어졌고, 하드웨어 보안이 신뢰 기반 컴퓨팅에서 어떤 역할을 하는지에 대한 논의가 있었다.

조수빈:
하드웨어 공격이 소프트웨어 공격에 비해 한계가 없다는 부분이 어떤 차이에서 이루어지는지에 대해 질문하였다. 하드웨어의 경우 한 번 출시되면 공격에 대한 패치가 불가하고 접근 제어나 권한 처리 같은 게 불가능하다는 부분에서 공격에 한계가 없다는 답변을 얻었다.

형유림:
내가 발표를 담당한 챕터 ‘하드웨어 암호학’이었다. SW 보안과 HW 보안의 개념을 설명한 후, HW 보안에서 주로 이용하는 모듈인 TPM과 HSM을 소개하였으며, 최근 HW 보안 위협 동향, 그에 따른 대응 전략 현황을 소개하고 HW 보안 시장의 향후 전망을 소개하며 마무리했다.</td></tr>
</table>

	No.	클럽원 정보	후기 내용
활동 후기	1	형유림 (2394016)	선정한 책 <리얼월드 암호학>이 생각보다 많은 내용을 다루면서도 어렵고 깊은 내용 또한 담고 있어서 공부하기에 아주 좋은 책이었던 것 같다. 보안 업계와, 더 나아가 IT 기술을 활용하는 전 산업에서 주시하고 있는 기술 동향과 각종 보안 사건사고를 책 한 권으로 공부할 수 있어서 좋았다. 우리 독서클럽은 세미나 형식으로 진행하여, 각 회차마다 한 명씩 한 챕터를 맡아 내용을 발표했어야 했는데, 지도교수님의 조언에 따라 기술의 원리 등보다는 해당 기술이 어느 분야에서 어떻게 쓰이고 있는지를 중점으로 발표 내용을 구성했다. 덕분에 이미 다 읽었을 책 내용에만 치중하지 않고, 보안이라는 게 실제로 전 산업과 전 업계에 걸쳐 얼마나 큰 중요도를 차지하고 있는지 알 수 있었다. 또한 각 발표 이후 교수님께서 피드백으로 알려주신 관련 업데이트 사항이나 관련 기술, 업계 동향, 더 공부하면 좋을 것 등은 아주 값진 정보였다. 이번 학기에 독서클럽 활동을 하길 정말 잘했다는 생각이 든다.
	2	김하경 (2394010)	리얼월드 암호학을 함께 읽으며 암호 기술의 원리뿐 아니라 실제 보안 환경에서의 적용 방식까지 깊이 있게 이해할 수 있었습니다. 각 회차마다 팀원들이 맡은 챕터를 핵심을 잘 짚어 설명해 준 덕분에 AES 구조, 암호화폐 분석, 하드웨어 보안 등 복잡한 개념도 훨씬 쉽게 다가올 수 있었습니다. 특히 발표 후 교수님께서 매번 꼼꼼하게 피드백을 주신 점이 매우 인상 깊었고, 핵심 개념을 다시 정리하고 더 깊이 사고해 보는 데 큰 도움이 되었습니다. 자유로운 질문과 토론을 통해 서로의 관점을 넓히고, 실무와 이론을 함께 이해할 수 있었던 뜻깊은 시간이었습니다.
	3	손채민 (2394032)	이번 독서클럽을 통해『리얼월드 암호학 이야기』를 읽으며 암호학의 다양한 분야에 대해 폭넓게 이해할 수 있는 계기가 되었다. 특히 나는 평소 블록체인 기술에 관심이 있어 암호화폐에 대해 발표를 준비하게 되었고, 이를 계기로 블록체인을 기반으로 작동하는 비트코인의 구조와 원리를 더 깊이 이해할 수 있었다. 책을 읽는 것뿐 아니라, 동기들의 다양한 발표를 통해 내가 몰랐던 암호학 분야도 접할 수 있었다. 예를 들어 AES의 암호화 원리, 양자컴퓨터 시대의 암호학, 그리고 하드웨어 기반 암호 기술 등은 기존에 생각하지 못했던 새로운 시야를 열어주었다. 발표를 듣는 과정에서 암호학이 단순히 이론에 머무는 것이 아니라, 현실 세계의 보안과 밀접하게 연결되어 있다는 점을 깨달았다. 무엇보다 이 시간을 통해 앞으로 내가 더 깊이 공부하고 싶은 분야를 구체화할 수 있었다는 점이 가장 큰 수확이었다. 암호학이 단순히 추상적인 수학이 아니라, 실제로 세상을 움직이는 기술이라는 사실이 인상 깊었고, 앞으로의 진로를 결정하는 데 있어서도 큰 도움이 되었다.
	4	조수빈 (2394025)	Real-World Cryptography는 현대에 자주 쓰이는 암호학과 최신 동향을 설명해주는 책으로, 보안 업계 전반을 살펴볼 수 있어 좋은 책이었다. 이번 독서클럽에서는 이 책을 기반으로 각자 원하는 챕터를 맡아 세미나 발표를 진행하는 형식으로 진행했다. 발표가 끝난 후에는 지도교수님께 피드백을 받는 방식으로 운영되었다. 나는 챕터 4, 인증 암호화 부분을 맡아서 그 중에서도 AES를 중점적으로 발표했다. 발표를 준비하는 과정에서 운영 모드와 암호화에 대한 혼동이 있었는데, 자료를 정리하고 교수님의 피드백을 받으면서 두 개념의 차이를 명확히 알 수 있어 도움이 많이 되었다. 다른 발표 중에서는 암호화폐에 대한 내용이 특히 인상 깊었다. 평소에 잘 이해가 되지 않았던 암호화폐의 구성과 채굴 과정, 그리고 암호화폐로 이루어지는 범죄를 어떻게 해결할 수 있을지에 대한 다양한 방안까지 생각해볼 수 있는 기회가 되어 유익했다. 전체적으로 책을 통해 암호의 최신 동향에 대해