47 유니티 멀티플레이어 환경에서의 경량 암호 통신 구현

소속 정보컴퓨터공학부 분과 D 팀명 민트초코펩시 참여학생 고세화, 김재민, 이강인 지도교수 손준영

연구 개요

연구 배경

게임 보안은 **해킹 방지**, **개인정보 유출 방지** 등 매우 중요

게임의 공정성을 해치는 **핵**

게임사의 **개인정보 유출**

연구 목표

☐ **MMORPG**(**M**assively **M**ultiplayer **O**nline **R**ole-**P**laying **G**ame) 게임 환경 **구현** (서버 – 클라이언트)

☐ **네트워크 보안**을 위한 다양한 **암호 알고리즘** 구현 (전자 서명, 키 교환, 블록 암호 및 운영모드 등)

☐ 게임 환경에서 **경량 암호 알고리즘**을 포함한 다양한 암호 알고리즘의 **성능 확인**

☐ **Handshake Protocol 설계** 및 **안전한 게임 통신 환경** 구현

구현 요약

☐ 고성능 서버(IOCP), 클라이언트(Unity), 소켓 통신
☐ **전자 서명** 알고리즘 ECDSA
☐ **키 교환** 알고리즘 ECDH
☐ **키 유도** 함수 HKDF
☐ **블록 암호** 알고리즘 AES, ARIA, HIGHT, SPECK, TWINE
☐ **블록 암호** 운영모드 ECB, CBC, CFB, OFB, CTR, GCM

연구 내용 및 시뮬레이션

암호 알고리즘

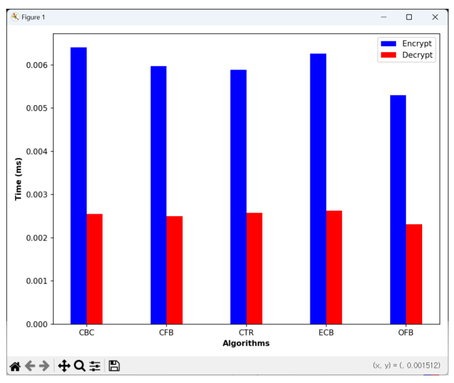
```
******* AES TEST START *******

[AES - ECB] [Success]    ECBGFSbox128.txt
[AES - ECB] [Success]    ECBKeySbox128.txt
[AES - ECB] [Success]    ECBMMT128.txt
[AES - ECB] [Success]    ECBVarKey128.txt
[AES - ECB] [Success]    ECBVarTxt128.txt

[AES - CBC] [Success]    CBCGFSbox128.txt
[AES - CBC] [Success]    CBCKeySbox128.txt
[AES - CBC] [Success]    CBCMMT128.txt
[AES - CBC] [Success]    CBCVarKey128.txt
[AES - CBC] [Success]    CBCVarTxt128.txt

[AES - CFB] [Success]    CFB128GFSbox128.txt
[AES - CFB] [Success]    CFB128KeySbox128.txt
[AES - CFB] [Success]    CFB128MMT128.txt
[AES - CFB] [Success]    CFB128VarKey128.txt
[AES - CFB] [Success]    CFB128VarTxt128.txt

[AES - OFB] [Success]    OFBGFSbox128.txt
[AES - OFB] [Success]    OFBKeySbox128.txt
[AES - OFB] [Success]    OFBMMT128.txt
[AES - OFB] [Success]    OFBVarKey128.txt
[AES - OFB] [Success]    OFBVarTxt128.txt

[AES - CTR] [Success]    CTR128.txt

[AES - GCM] [Success]    gcmDecrypt128.txt
[AES - GCM] [Success]    gcmEncryptExtIV128.txt

******* AES TEST END *********
```

☐ 다양한 암호 알고리즘을 **표준**에 맞게 구현

☐ **테스트 벡터**를 통한 검증

☐ **ECDSA, GCM** 등 강력한 암호 알고리즘 포함

성능 측정

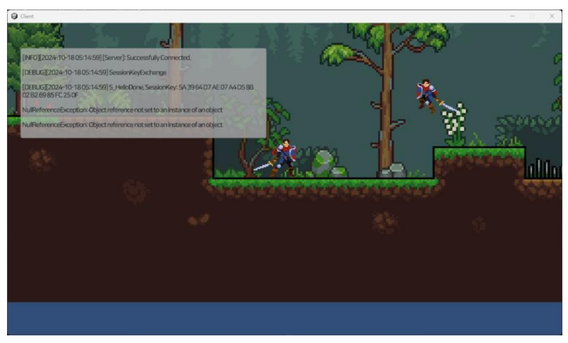


☐ 블록 암호, 운영모드 **시간 측정**

☐ **SPECK-CBC**가 가장 빠름

☐ **GCM**의 경우 암호 알고리즘과 무관하게 0.1ms 이하

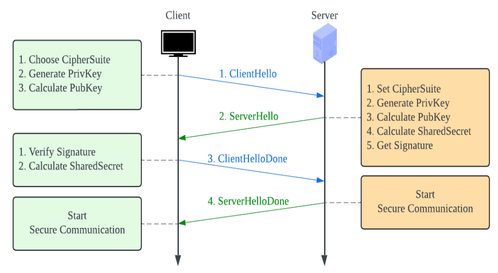
게임 환경



☐ 클라이언트: **Unity**

☐ 서버 : C# **IOCP** (고성능, 비동기)

Handshake



☐ **TLS 1.3**을 참고한 설계

☐ 서버 **인증**, **키 교환**, **키 유도** 과정 포함