Team No.

TONGMYONG UNIVERSITY

전공연구형_Capstone Design 신청서

과제명	국문	난수를 이용한 암호 생성 프로그램 구축					
	영문	Constructing a password generation program using random numbers					
과제팀명		CDT(Capstone Design Team)					
참여학과		정보보호학과	교과목명		DID 인증 기술 _Capstone Design		
지도교수		성명				소속(학과)	
		신 승 수				정보보호학과	
참여 학생	구분	소속학과(전공)	학번	학년	성명	연락처	이메일
	팀장	정보보호학과	18학번	3	손 * *	010-4949-****	nmama8484@naver.com
	팀원	정보보호학과	20학번	3	양 * *	010-5622-****	alfo6715@naver.com
		정보보호학과	20학번	3	임 * *	010-6391-****	lgusdk04@naver.com
		정보보호학과	19학번	3	이 * *	010-9343-****	dldbswn0311@naver.com
수행기간		2022년 9월 14일 ~ 2022년 12월					
유형선택		☐ 기업성장형 ☐ 사회기여형 ☐ 창업연계형					
구분 / 지원금액		■ 전공연구형	☐ 과제창출형_C유형 (예산 300,000원)				
			■ 학술연구형_D유형 (예산 200,000원)				

동명대학교 현장실습지원센터 규정에 의거, 캡스톤디자인 과제를 성실하게 수행하고자 본 과제 신청서를 제출합니다.

붙임 : 과제 제안서 1부

2022. 9. 14.

신청인(대표학생) : 손 * *(인)

과제지도교수 : 신 * *(인)

동명대학교 현장실습지원센터장 귀하

<별지 제4호 서식> (개정 2018.03.12.) (2019.09.20.) 전공연구형

Capstone Design 과제 제안서

1. 과제 선정 배경 및 과제 수행 목적

- 암호를 설정할 때 사람들은 무의식적으로 자신과 관련된 영문, 숫자들을 기입하는 편이고 개인 PC 및 각종 웹 사이트 암호를 하나로 통합하여 쓰며 해커의 입장에서 해킹을 시도할 때 그러한 암호들을 먼저 공격한다.
- 아무리 교묘하게 암호를 만든다 해도 컴퓨터는 사람이 생성한 암호를 쉽게 추측이 가능하며 영문 대소문자, 숫자, 특수문자를 조합하여 암호를 생성한다면 안전성이 확보된다.
- 암호에 대한 모범 사례, 위치, 값 및 보안 고려 사항이 복잡성 요구 사항 보안 정책 설정을 충족해야 하며 그에 따른 내용들을 숙지하며 암호에 대한 중요성을 깨달을 필요가 있다.
- 현재 사용되고 있는 암호체계는 수학적 복잡성에 기반을 두고 있고 가역적이기 때문에 언젠가는 암호가 풀리게 된다.
- 가장 강력한 암호체계 중 하나로 불리는 RSA의 경우에도 문제 풀이에 천문학적인 시간이 소요되지만 결국엔 풀린다.
- 그에 따라 암호를 더 어렵고 복잡하게 설계를 해야 하기에 16자리 이상의 난수를 사용하여 암호를 강력하게 만들어야 한다.
- 난수는 무작위성, 불규칙성, 우연성 이 3가지 요소를 충족하여야 한다.
- 영문 대소문자, 숫자, 특수문자를 활용하여 일정 길이의 난수를 생성하는 프로그램을 구축하고자 한다.
- C언어를 통해 구축을 하며 파이썬을 통해서 서로 어떻게 다른 차이점이 있는지에 대해 알아보고 가장 효율이 좋은 방식을 찾고자 한다.

2. 과제 수행 방법

- 과제를 진행하며 난수의 생성 과정과 난수에 대한 정의를 정리하며 주제에 대한 이해도를 높일 계획임.
- 난수 생성에 필요한 rand, srand, time 함수에 대한 이해 진행.
- 난수 생성기에 대한 코드는 C언어로 작성을 하며, 파이썬으로도 코드를 작성해 보고 C언어 코드와 비교하였을 때 어떤 방식이 더 효율성이 높은지 비교함.
- 실제로 난수 생성기를 돌려보며 규칙성이 생기는지 확인을 진행함.
- 난수의 규칙성 제거를 위해 seed 값을 변경하여 난수 값이 균일하게 분포되었는지 확인함.

3. 결과물에 대한 기대효과 및 활용방안

- 난수 생성기로 인해 발생하는 암호는 무차별 대입 공격(brute-force-attack)에 의해 언젠가는 풀리겠지만 천문학적인 시간이 소요될 것으로 추정됨.
- 해당 암호를 기억하기 위해서는 메모 및 저장을 해야 하겠지만 그 문서만 잘 보관한다는 가정하에 안전한 암호라고 볼 수 있음.
- 난수를 암호로 설정하여 단순한 암호 설정으로 인한 해킹 사례를 감소시켜 줄 것임.
- 영문 대소문자, 숫자, 특수문자를 이용해 무작위 암호 생성기로 만든 암호는 쉽게 추측하기 어렵고 암호 해독도 어려워 강력한 암호가 될 것임.

4. 수행 일정

주요내용	추진일정			소요 기간(월)
	09	10	11	
Brainstorming				*1주*
난수에 대한 이론지식 습득				*1개월*
자료수집				*2주*
연구에 필요한 언어 숙지				2개월
프로그램 제작 및 구현				1주

5. 팀원별 역할

No.	성 명	담당 및 수행업무
1	**손 * ***	**보고서, 회의록 작성 및 자료 정리, 수집**
2	**양 * ***	**난수에 관한 정의 및 자료수집**
3	**임 * ***	**C언어 및 파이썬을 이용한 난수 생성 과정 코드 분석**
4	**이 * ***	**C언어 및 파이썬의 효율 정리 및 결과물에 대한 활용방안 정리**

6. 소요 예산

구분	용도 (과제수행과의 연관성)	품목	규격	단위	수량	단가	금액 (원)
재료비							
그 외	용도 (과제수행의 연관성 기술)			산출 내역			금액 (원)
회의비	과제 수행 팀원과의 회의 진행			주 1회 한정			(4000원 * 인원)
⋮							
합 계				원			