Proposed by
Free'C'ize

BUSINESS PROPOSAL

2021

Free'C'ize

PM. Keon-hee Choi.
PL. Yong-jin Lee.
PL hyeon-ho Lee.

Intern.
Yoon-seo Ki.
Dong-chan Kim.

Oct, 20 2021

Project No. 1

About the Team

We made EntersStellar!
We provide crypto libraries

Company team members

Project Manager

Keonhee Choi

Project Leader

Yong-jin Lee

hyeon-ho Lee

Intern

Yoon-seo Ki

Dong-chan Kim

우리는 국민대학교 고급응용프로그래밍 수업에서 배운 큰 정수 연산을 구현하기 위해 만들어진 팀입니다.

각자의 다른 관심사와 다양한 분야에서의 경험을 하나로 모아 “EntersStellar”를 제작하였습니다.

다양한 암호 구현에서 이용 될 수 있는 “EntersStellar”는 Cyber-Security한 세상을 만드는데 큰 역할을 할 것입니다.

우리 팀의 이름은 다음과 같은 의미를 지니고 있습니다.

Freesize는 자신의 몸집에 상관없이 자유롭게 입을 수 있는 옷을 의미합니다.

하지만 C언어는 자료형의 크기가 한정되어 있어 특정 값 이상은 저장할 수 없습니다.

암호 구현에도 자유롭게 입고 쓸 수 있는 옷, 즉 라이브러리가 있다면 어떨까요?

저희 팀 Free’C’ize는 이런 한정성에 착안하여 수의 크기에 상관없이 값이 저장 될 수 있는 옷, 즉 큰 정수 라이브러리 “EntersStellar”를 제작합니다.

Free’C’ize의 EnterStellar는 현대 암호에서 요구되는 큰 정수 연산과 학생들을 위한 암호교육에 활용될 것입니다.

Keonhee Choi
Project Manager

제안 배경 및 필요성

c언어에서 기본적으로 제공하는 자료형은 큰 수 담거나 연산하는데에 한계가 있습니다.
이에 우리는 사용자가 원하는 큰 수를 입력 받아서 연산이 가능한 라이브러리를 제작하고자 합니다.
큰 수를 다루어야 하는 상황은 다양하지만 본 프로젝트에서는 암호알고리즘에 초점을 두고 개발을 진행합니다.

RSA, DSA등 여러 암호 알고리듬에서 매우 큰 소수를 사용하는 경우가 많다.
그러한 소수를 다루기 위해서 Big number Library 라이브러리가 필수적으로 이용된다.
이때의 소수를 생성하기 위해 밀러-라빈 test를 구현할 것입니다.
또한 파일 암호화까지 확장시켜서 다양한 암호 알고리즘에 이용될 수 있도록 개발할 계획을 가지고 있습니다.

본 라이브러리의 이름 EnterStella의 stellar는 '항성간의 별들의' 뜻을 가지고 있습니다.
우리는 우주의 수많은 항성의 개수만큼 큰 빅넘버를 사용할거라는 의미에서 그 항성들 사이로 여행을 해보는 의미로 EnterStellar라 명명하게 되었습니다.

구현방안 및 아이디어

EnterStellar Library의 헤더파일 및 함수들 소개

1) E_Core: 큰 수를 다루기 위해 기본적으로 필요한 함수들의 모임(생성자, 제거자, Refine, show, assign 등).
추후 연산에 필요한 다양한 기초적인 함수를 구현할 계획이 있다.

2) E_operation: E_add, E_sub, E_mul, E_div, E_shift (덧셈, 뺄셈, 곱셈, 나눗셈, 쉬프트연산 등)을 구현할 계획이 있다. 효율적인 사칙연산과 쉬프트연산을 통해 추후에 암호에 용이하게 사용 가능하도록 만들 것이다.

3) E_prime: Is_prime, make_prime 등 소수와 관련된 함수들을 만들 계획이다.
이때의 소수 판별법으로는 밀러라빈 Test를 사용할 것이고 판별횟수의 제한은 NIST의 표준문서를 따를 계획에 있다.

4) E_cryptoalg: E_RSA_n(n은 bit 크기 자유자재로 조절가능하게 n = 1024, 2048등),
E_DSA(전자서명 함수)를 구현할 계획에 있다.

Code - Test

테스트 방법은 두가지 중 하나로 진행할 예정입니다.

File Input/Output : 파일 입출력을 통한 Data set 생성과 검증 방법

1. 두개의 랜덤한 Bigint를 생성합니다.
2. 두개의 Bigint로 원하는 연산(ex : Addition, Subtraction, Multiplication, etc)을 진행하여 새로운 Bigint를 생성합니다.
3. 두개의 Bigint와 연산하여 출력된 Bigint를 파일 입출력(ex : .txt, .csv, .xlsx …)을 통하여 Data set을 만듭니다.
4. 1 ~ 3의 과정을 반복하여 적당한 크기의 Data set을 만듭니다.
5. 파이썬(or sage)으로 Data set을 읽어드립니다.
6. 파이썬(or sage)으로 연산을 진행하여 정확한 값이 나오는지 확인합니다.
7. 모두 정확하다면 검증 통과하고 하나라도 실패한다면 검증 실패합니다.
8. 검증 확인은 조건문과 반복문을 활용하여 처리할 생각이며 검증 진행도를 알기 위해 10개를 검증할 때마다 진행도(ex : 30 %)를 출력합니다. 정확도 또한 출력합니다.

1번의 검증 방식은 Data set의 크기만큼 용량 차지가 발생하고 Data set을 얼마나 크게 만드는지에 따라 파일 생성에 시간이 걸릴 수 있다는 단점이 있습니다. 하지만 한번 만들어 두면 나중에 Bigint 연산의 고속화를 위한 Table Look Up 방식에 도움이 될 수 있다는 장점이 있습니다.

Code - Test

테스트 방법은 두가지 중 하나로 진행할 예정입니다.

Embedding Python in C : C언어에 파이썬을 임베딩하여 검증하는 방법

1. Python.h를 include하여 C언어에서 파이썬을 사용할 수 있도록 합니다.
2. sage 패키지를 파이썬에 import 합니다.
3. 파이썬에서 Bigint 연산을 검증하는 함수를 생성합니다.
4. Python.h를 include한 C파일에서 파이썬에서 작성한 검증 함수를 불러옵니다.
5. 파일에서 랜덤하게 생성한 두개의 Bigint와 연산 출력 값을 파이썬 함수에 파라미터로 넣어 검증합니다.
6. 5번의 과정을 반복적으로 시행합니다.
7. 한번이라도 틀린다면 검증 실패입니다.
8. 마찬가지로 검증의 진행도와 정확도를 출력합니다.

2번의 방법은 C언어에 파이썬을 임베딩하는 과정이 복잡하고 어려워 테스트 설정하는 것이 시간이 오래 걸린다는 단점이 있습니다. 하지만 한번 테스트 설정을 해 두면 여러 개를 검증할 수 있을 뿐만 아니라 하나씩 검증하는 것 또한 가능합니다. 그리고 파일 입출력을 하지 않아 하나의 C파일에서 한 번에 검증이 가능합니다.

파급효과

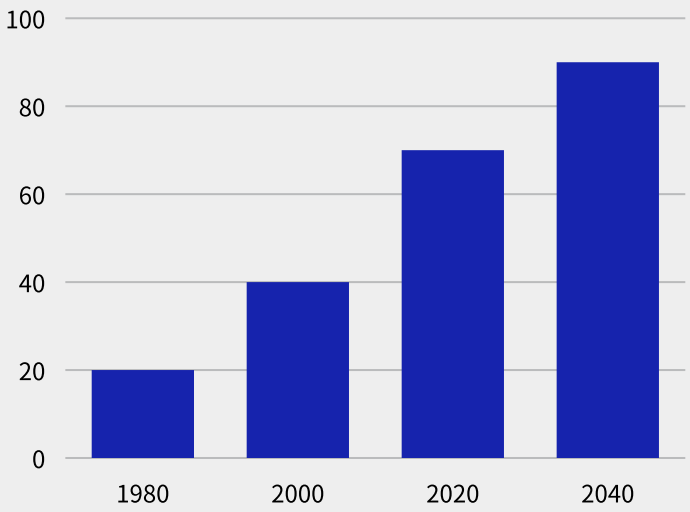
암호 구현의 용이성

EnterStellar Library를 통해서 RSA, DSA 암호 구현에 도움을 줄 수 있음을 보일 수 있습니다. 추후 RSA, DSA 이외에도 다양한 암호 구현에 이용될 수 있으므로 유용한 라이브러리가 될 것입니다.

암호 대한 대중성 & 친근감 형성

암호에 대한 친근감을 대중에게 제공하고 암호의 필요성 등을 구체적으로 보일 수 있는 기회입니다. 대학생인 우리가 직접 만든 Enterstellar Library통해 암호를 구현하고 이를 학생의 눈으로 알리는 것은 암호의 대중성을 높이는 것이라고 생각합니다. 따라서 추후 암호 라이브러리와 기초 암호에 대한 홍보를 다양한 채널을 통해서 할 계획을 가지고 있습니다. 포스트 코로나 시대의 사회활동을 할 수 있는 공간을 제공합니다. 우리는 EnterStellar를 활용해 암호를 이용한 사이버 보물찾기등 현장에 참여하기 힘든 사람들을 위해 사이버 행사를 진행하는 방법을 제시합니다. 이를 통해 사람들에게 자연스럽게 다가갈 수 있을 것입니다. 또한 대중들이 암호에 대한 쉬운 접근이 가능해 질 것입니다.

암호에 대한 대중의 관심도예측



PRICE

본 라이브러리를 통해 학생들에게 교육을 제공하는 단순한 게임을 기획하고 있습니다. 현제 다양한 후보군들이 있으며, 한가지의 후보를 소개하고자 합니다.

[GAME] 보물 찾기

기존 암호에 관해 관심을 갖게하기 위해 RSA-16bit 를 이용한 보물찾기 게임을 제안합니다. 우리는 여러 공개키와 비밀키 쌍을 제공하는 기능을 만들어 제공합니다. 운영진들은 상품(경품등)과 꽝 등 을 공개키로 암호화한 후 특정 인스타그램, 카페,블로그 등에 숨겨둔다. 이때 비밀키 또한 랜덤하게 숨겨두게 됩니다. 운영진들은 플레이어들에게 RSA 암호화를 복호화 할수 있도록 우리 라이브러리를 배포합니다. 비밀키를 찾아 숨겨진 보물을 획득하는 것이 핵심입니다. 또한 비밀키를 추측해서 상품을 얻을수 있다는 사실은 보안에서 빅넘버의 중요성을 플레이어들에게 인식시켜줄수 있습니다. 이렇게 자연스럽게 암호에 관심을 갖게 하는 계기가 될 것이라고 기대합니다. 마치 복권을 동전으로 긁었을 때 어떤 상품이 있을지 기대되는 그런 희열감 등을 느끼게 하는 것이 우리의 목적입니다.

우리는 암호의 발전과 더불어 안전한 사이버 방역을 위해 힘쓸 것입니다. 또한 학생들에게 암호와 그 중 빅넘 라이브러리의 중요성을 알려주며 먼 미래의 세상에 투자 할 것입니다. 따라서 저희의 라이브러리 가격은 무료입니다. 우리는 전 세계인의 개인정보가 안전하게 보호되고 마음 편히 놀 수 있는 사이버 세상에 투자한 것입니다. 저희 제안서를 읽어 보시고 동참해주신다면 감사하겠습니다.