대칭키 암호 알고리즘

컴퓨터SW 18017103 황제현

목 차

아이디어 개요

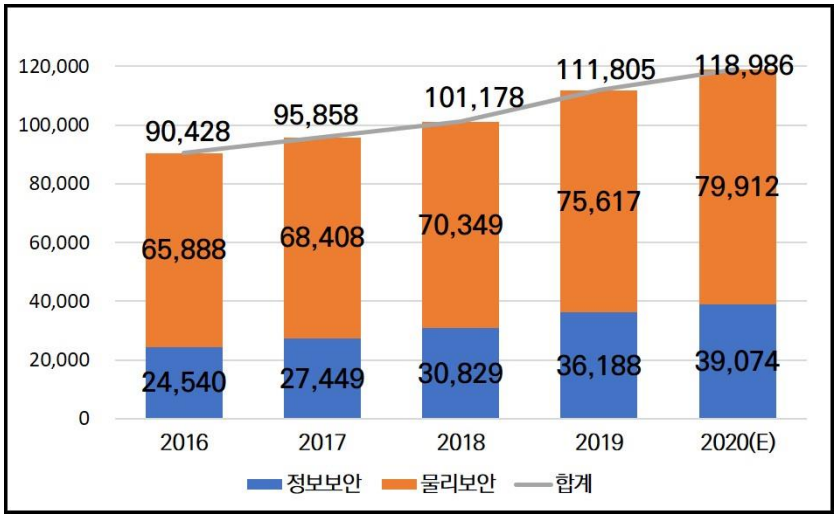
프로그램 흐름도

기대 효과

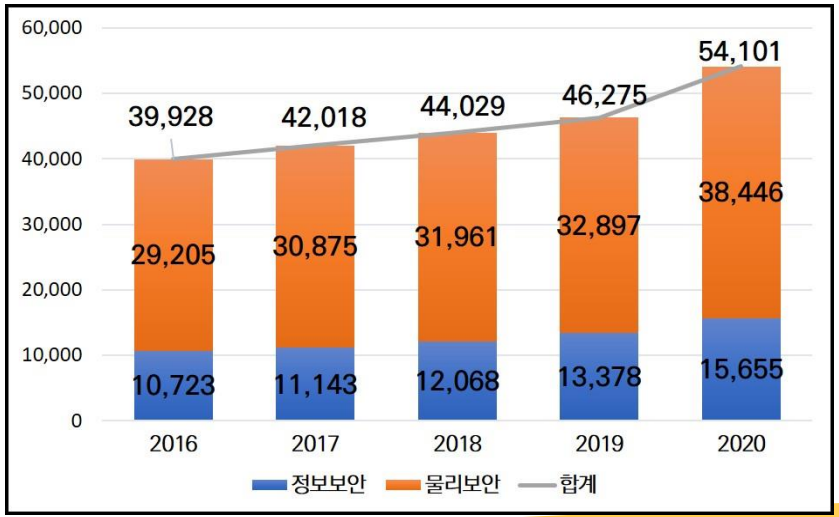
1. 아이디어 개요

1. 아이디어 개요

4차 산업혁명, 코로나 등으로 인한 디지털 전환 가속으로 IT산업의 규모가 커짐에 따라, **정보보안의 중요성** 또한 날로 증대하고 있다.



국내 정보보호산업 매출액(백만원)
(2020 국내정보보호산업 실태조사, 한국정보보호산업협회)

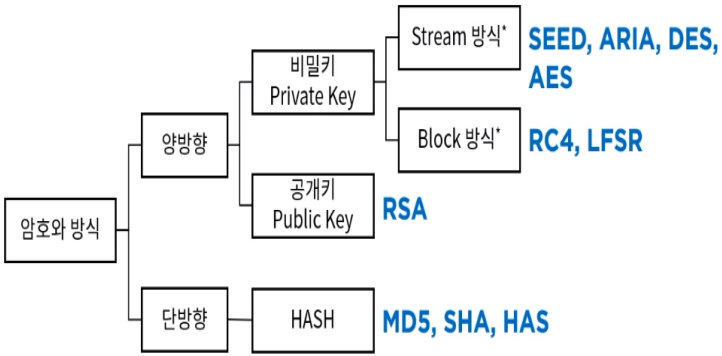


국내 정보보호산업 인력현황(명)
(2020 국내정보보호산업 실태조사, 한국정보보호산업협회)

1. 아이디어 개요

정보보호 제품 이용률
(2020 정보보호 실태조사, 한국정보보호산업협회)

기업, 단체, 개인 상관없이 자신의 정보를 지키는 것은 선택이 아닌 **필수**가 되었다.



여러가지 암호화 방식
([보안] 암호 알고리즘 (Encryption Algorithms) (velog.io))

우리가 이용하는 보안제품이나 각종 서비스의 보안 기능의 핵심은 **데이터 암호화**이며, 여러가지 기법이 존재한다.

1. 아이디어 개요

이번 프로젝트의 목표는 대칭키 암호 알고리즘을 이용하여 간단한 **암호화 프로그램**을 구현하는 것이다.

대칭키 암호 알고리즘은 데이터를 암호화, 복호화 할 때 **동일한 키**를 사용하는 방식이며, 특징은 다음과 같다.

장점

- 암호/복호화 속도가 빠름
- 알고리즘이 단순함
- 파일의 크기가 작음

단점

- 사용자가 많아지면 관리해야 할 키도 늘어남

1. 아이디어 개요

문제점 - 키의 배송 문제

아무리 알고리즘을 강력하게 설계해도,
암호화의 핵심인 **키를 도난** 당하면 아무 소용이 없다.
따라서 **키를 안전하게 전달하는 것이 중요**하다.

해결방안

1. **키를 별도로 암호화** 한다. 이 방식을 발전시키면 공개키 암호화 방식이 된다.

2. 통신 시마다 **키를 새로 생성**한다. (일회성 대칭키) 유사한 개념으로 OTP가 있다.

예시) 토큰 방식의 OTP 발급기

2. 프로그램 흐름도

2. 프로그램 흐름도 (암호화)

* 과정 도식화를 위해 연출한 실행결과로, 실제와 다를 수 있음.

1. 데이터를 입력받는다.

suction
2735

2. 데이터를 유니코드로 변환한다.

115 117 99 116 105 111
110 32 50 55 51 53

3. 키를 생성하고 XOR연산한다.

115 117 99 116 105 111 110 32 50 55 51 53
XOR
41 76 47 15 0 114 31 110 23 41 67 77
=
90 57 76 123 105 29 113 78 37 30 112 120

3. XOR연산 결과를 무작위 진법으로 변환한다.

ex) 8진법
132 71 114 173 151 35 161 116 45 36
160 170

5. 연산결과를 다시 문자열로 변환한다.

□G r □# ¡ t - $ ª

2. 프로그램 흐름도 (복호화)

* 과정 도식화를 위해 연출한 실행결과로, 실제와 다를 수 있음.

1.변환된 문자열과 키를 전달받는다.

□G r □# ¡ t - $ ª
Key = 41 76 47 15 0 114 31 110 23 41 67 77
진법 = 8

2. 문자열을 다시 유니코드로 변환한다.

132 71 114 173 151 35 161 116 45 36 160 170

3. 유니코드는 8진법으로 변환된 상태이므로 10진수로 다시 변환한다.

90 57 76 123 105 29 113 78 37 30 112 120

4. 키와 다시 XOR연산한다.

90 57 76 123 105 29 113 78 37 30 112 120
XOR
41 76 47 15 0 114 31 110 23 41 67 77
=
115 117 99 116 105 111 110 32 50 55 51 53

5. 문자열로 변환한다.

suction 2735

3. 기대 효과

3. 기대 효과

- 개발 역량 강화

- 암호 알고리즘의 원리를 이해하고 직접 파이썬으로 구현함으로써 관련 지식을 학습하고 개발 역량을 강화할 수 있다.

- 이식성

- 데이터 자체를 암호화하는 방법을 제공하므로 데이터를 다루는 모든 분야에서 광범위하게 활용할 수 있다.