|  |
| --- |
| **정보보호 과제 리포트**  암호화 기법 조사 (대칭키, 비대칭키) |



|  |  |  |  |
| --- | --- | --- | --- |
| 제출일 | 2021. 12. 05 | 전공 | 컴퓨터정보공학전공 |
| 과목 | 정보보호 | 학번 | 2123405 |
| 담당교수 | 이수철 | 이름 | 최창환 |

|  |
| --- |
|  |

**정보보호 과제 리포트**

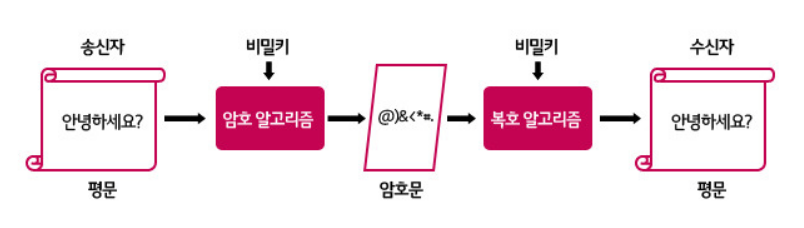
**1. 암호화 기법**

데이터를 보낼 때 데이터가 변경되거나 손실되는 것을 방지하기 위해 데이터를 변환하여 전송하는 방법.

**2. 대칭키와 비대칭키**

암호화 기법에는 크게 두 가지가 존재 한다.

**2-1. 대칭키 암호화 방식**



전자 문서나, 메일이 대칭키로 암호화된다면 똑같은 대칭키를 가지고 있는 사용자만이 문서를 복호화 할 수 있는 방식을 말한다. 누군가 암호화된 전자문서를 받게 되어도 이를 해독하지 못하기 때문에 발견한 사람에게는 아무의미가 없는 문서가 될 수 있다는 장점이 있다. 하지만 이러한 방식에도 단점이 존재한다.

하나의 비밀키를 (Client - Server) 가 모두 같이 사용하는 것이다. 즉, 비밀키를 하나만 알아내면 암호화된 패킷을 모두 해독이 가능하기 때문에 해커로부터 안전 할 수 없다.

대칭키 암호화 방식은 데이터를 변화하는 방식에 따라 블록암호(AES)와 스트림 암호로 구분된다.

블록 암호 같은 경우 평문을 블록 단위로 나눠 키와의 연산을 통해 암호화를 수행하는 방식이며, 스트림 암호는 유사 난수를 연속으로 생성하여 평문과 유사 난수와의 연산을 통해 암호화를 수행하는 방식이다.

**- 원리**

암호화와 복호화에 두 개의 서로 다른 키를 사용하는 암호 방식이다.

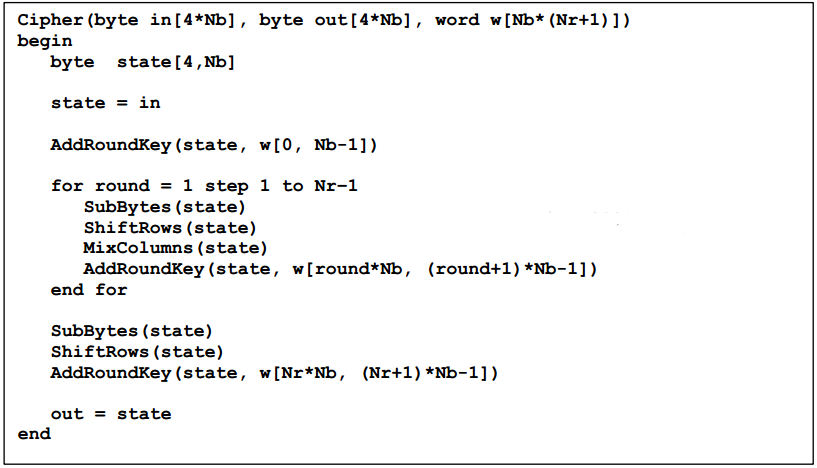
**- AES 암호 알고리즘 (왼쪽: 암호화, 오른쪽: 복호화)**



고급 암호화 표준(Advanced Encryption Standard)이라고 불리는 AES 암호 알고리즘은 DES를 대체한 알고리즘 이며 암호화와 복호화 과정에서 동일한 키를 사용하는 대표적인 대칭키 알고리즘이다. DES에 비해서 가변 길이의 블록과 가변 길이의 키 사용이 가능하며, DES와는 다르게 SPN 구조를 사용한다.

AES 알고리즘 라운드 내부에서는 4가지 연산이 존재한다. 치환 연산과, 단순 자리바꿈을 위한 Shift 연산, 기약 다항식 계산을 위한 연산, 마지막으로 xor을 활용한 키 값을 구하는 연산이 있다.

**- 암호화(encryption) C++ 의사 코드**



① S-box transformation-SubBytes()

- 각 바이트에 대해 처음 4bit는 16진수 x를 라인 번호로, 마지막 4bit는 16진수 y를 컬럼 번호로 대입한다.

② Line transformation - ShiftRows()

- 첫 번째 행은 그대로, 두 번째 행은 왼쪽으로 1bit, 세 번째 행은 왼쪽으로 2bit, 네 번째 행은 왼쪽으로 3bit 이동한다.

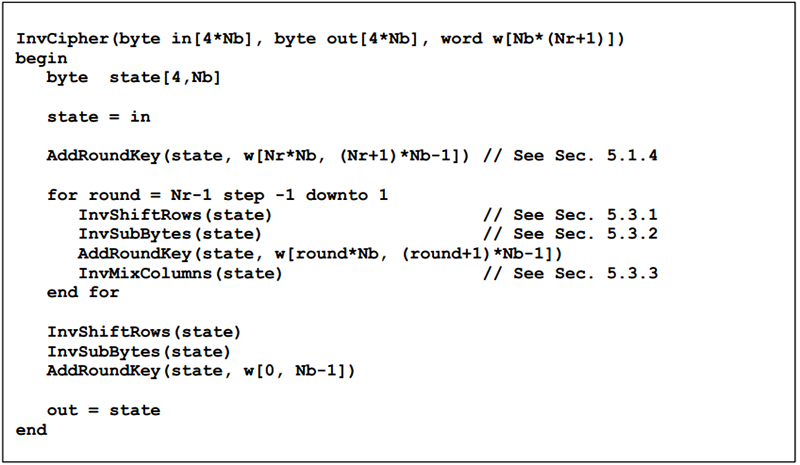
③ Column transformation - MixColumns()

- 4x4 바이트 행렬을 입력으로 받아 행렬을 열별로 변환한다.

④ XOR-AddRoundKey() with Extended Key

- xor 연산으로 라운드 키를 추가한다.

**- 복호화(decryption) C++ 의사 코드**



① Inverse transformation - InvShiftRows()  
- 행렬의 각 행에 대한 왼쪽 순환 이동과 오른쪽 순환 이동을 진행한다.

② Inverse S-box transformation-InvSubBytes()  
- InvShiftRows() 함수와 마찬가지로 동일한 방식으로 테이블을 순회한다.

③ Inverse transformation - InvMixColumns()

- xor 연산을 이용하여 각 컬럼 값을 변경한다.

**- DES 암호 알고리즘**

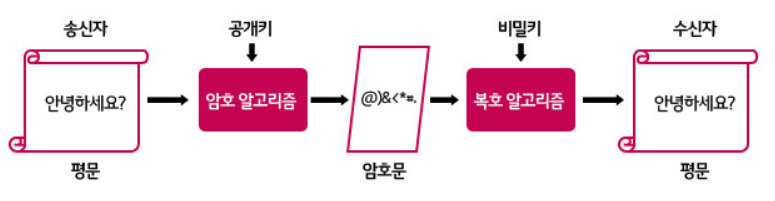
DES 알고리즘은 암호문을 작성할 때 사용하는 암호키와 암호문을 해독할 때 사용하는 해독키가 같다.

따라서 이 키는 절대로 외부에 유출되지 않도록 관리해야하며 비밀키(Secret Key)라고 부른다. 또한 양쪽이 동일 키를 사용한다고 해서 대칭키(Symmetric Key)라고도 한다. 이처럼 외부 사용자에게 노출되지 않아야하는 암호키로 암호화하는 알고리즘을 비밀키 알고리즘이라고 한다.

**- DES 알고리즘의 동작과정**



**2-2. 비대칭키 암호화 방식**



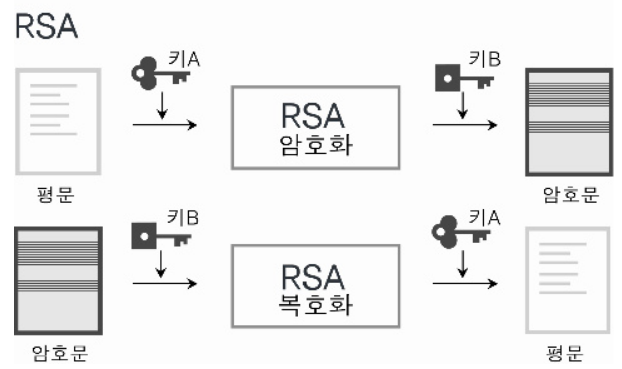
암호화 할 때 사용하는 키와 복호화 할 때 사용하는 키가 다른 경우를 의미한다. 비대칭키(공개키)암호는 대칭키 암호의 키 전달에 있어서 취약점을 해결하고자 한 노력의 결과로 탄생한 암호 방식이다. 비대칭키(공개키)암호는 한 쌍의 키가 존재하며, 하나는 특정 사람만이 가지는 개인키(비밀키)이고 다른 하나는 누구나 가질 수 있는 공개키를 가진다.

**- 원리**

보내야 하는 데이터를 송신자가 수신자의 공개키로 암호화를 걸어 놓고 데이터를 받은 수신자가 자신의 비밀키로 복호화를 하는 방법이다. 비밀키는 한쪽에만 속해 있기 때문에 비밀키가 사용된 것으로 나타난 모든 경우 해당 키는 소유자만이 그것을 사용했다고 할 수 있다.

**- RSA 알고리즘**

RSA 공개키 암호화 알고리즘의 기본 형태는 DES 같은 대칭키 암호화 알고리즘과 같다. 대칭키 암호화와의 차이점은 암호화 하는 키와 복호화 하는 키가 다르다는 것 밖에 없다. 기본적인 구조는 같지만 암호화 키와 복호화 키를 다르게 하기 위해 DES 알고리즘과는 확연히 다른 함수를 가지고 있다.



RSA 알고리즘의 형태는 위 그림과 같이 간단하게 구성 되어있다. 이 형태를 이용해서 키 교환이나 서명/인증과 같은 매커니즘을 구현 할 수 있다. RSA 알고리즘은 서로 다른 키를 가지고 데이터 암호화/복호화를 하는 것이 기능의 전부이지만, 이 특성을 이용해서 키 교환이나 서명/인증 등의 알고리즘을 구현 할 수 있다.

**- 일방향 함수**

모든 공개키 암호화 알고리즘은 일방향 함수를 사용한다. 일방향 함수라는 것은 한쪽으로는 계산이 수월한 반면, 그 반대쪽은 연산이 매우 어려운 함수를 의미한다. 암호화한 키는 일방향 함수를 이용해서 평문을 암호화 한다. 일방향 함수의 특징 상 반대쪽으로는 계산할 수 없으므로 암호문을 평문으로 바꿀 수 는 없지만 나머지 다른 하나의 키를 이용하면 역 변환을 쉽게 할수 있게된다. 나머지 키는 반대쪽으로 변환하는 역변환 함수의 열쇠 역할을 하는 것이다.

**3. 결론**

|  |  |
| --- | --- |
| 대칭키 암호 | 비대칭 키 암호 |
| - 암호화/복호화에 동일한 키와 알고리즘이 사용된다. | - 암호화/복호화에 동일한 알고리즘을 사용하지만 서로 다른키를 이용한다. |
| - 수신자와 송신자는 키를 교환해야 한다. | - 수신자와 송신자 사이에 키 교환이 필요없다. |
| - 공유한 키(비밀키)는 보안이 유지된다. | - 하나의 키(개인키)의 보안이 유지된다. |
| - 키의 분배가 어렵다. | - 공개키만 공유하면 된다. |
| - 속도가 비대칭키 방식에 비해 상당히 빠르다. | - 속도가 대칭키 방식에 비해 상대적으로 느리다. |

비대칭키 방식의 암호화 알고리즘이 대칭키 방식에 비해 상대적으로 보안에 취약하다는 단점이 존재하지만 비대칭키 암호화 알고리즘(RSA)이 이해와 구현이 쉽기 때문에 통상적으로 많이 쓰이고 있다.