암호 응용 및 실습

**HW1**

**제출기한: ~5/22 18:00**

**총점: 100 점**

| **이름** | 이혜린 |
| --- | --- |
| **학번** | 20190937 |

<참고사항>

* 제출 기한이 5/22 18:00 이므로 LMS의 과제 제출 란에 제출 시간전까지 업로드
* 지각 제출: 5/23 18:00 까지 허용. 채점 점수의 50% 만 인정 (예: 100점 만점이더라도 반영 점수는 50점)
* 1분이라도 늦게 제출 시에는 지각 제출이 되니, 반드시 제출 시간 준수
* 지각 제출 시에 감점이 크므로 반드시 제출 기한 내에 제출 바람
* Copy 시 점수 없음 (협업 시에도 본인이 직접 과제를 수행해야 함, 협업 시에 과제에 반드시 명시)

<제출 방법>

* 이론 부분 과제는 과제 답변 작성 후에 MS word 파일로 제출
* 실습 부분 과제는 .ipynb 파일로 제출 양식에 맞추어 제출

[암호의 기초]

1. 공격 모형 (Attack Model)을 정의하고, 공격 모형의 목표 세 가지에 대해서 설명하여라 [5점]

공격 모형: 공격자들이 암호와 어떠한 방식으로 상호작용하는지, 어떤 일들을 할 수 있는지에 대한 가정들의 집합

공격 모형의 목표:

* 암호를 설계하는 암호학자를 위해 어떤 공격자들과 어떤 종류의 공격들로부터 암호를 보호해야 하는지 알 수 있는 요구조건들을 설정한다.
* 사용자의 환경에서 암호가 안전할지 평가할 수 있는 지침을 사용자에게 제공한다.
* 암호를 깨고자 하는 암호 해독가를 위해 주어진 공격이 유효한지 알 수 있는 단서를 제공해준다.

1. 블랙박스 모형의 네 가지 종류를 나열하고 각각에 대해 설명하여라 [5점]
2. 암호문만 공격하는 모형 (ciphertext-only attackers, COA)

암호문만 알고 해당 평문을 알지 못한다.

암호화와 복호화 질의를 수행 못하는 수동적 공격자

1. 알려진 평문을 공격하는 모형 (known-plaintext attackers, KPA)

암호문과 해당 평문을 알 수 있다.

평문 - 암호문 쌍들을 얻을 수는 있지만 평문은 무작위로 선택되는 수동적 공격자

1. 선택된 평문을 공격하는 모형 (chosen-plaintext attackers, CPA)

자신이 선택한 평문에 대한 암호화 질의 수행이 가능하다.

능동적 공격자

1. 선택된 암호문을 공격하는 모형 (chosen-ciphertext attackers, CCA)

암호화와 복호화를 모두 할 수 있는 능동적 공격자

하지만 복호화 할 수 있다고 해서 반드시 주어진 시스템을 깰 수 있는 것은 아니다.

공격자가 원하는 것은 해독된 영상이 아니라 암호화에 사용된 비밀키를 알아내는 것이다.

1. 의미론적 보안에 대해 설명하고, 무작위 암호화가 필요한 이유에 대해서 설명하여라 [5점]

의미론적 보안이란 키의 비밀이 유지되는 한 공격자가 암호문으로부터 평문에 관해 어떤 정보도 알아내지 못해야 한다는 보안 목표이다.

무작위 암호화가 필요한 이유는 암호화가 무작위하지 않는다면 CPA 모형에서 공격자는 암호화 질의를 수행할 수 있으므로 주어진 암호문이 어떤 것과 같은지를 알아낼 수 있게 된다.

[고전 암호]

1. 모듈로를 30으로 하는 곱셈 암호에서 좋은 키가 될 수 있는 것을 모두 찾고 그 이유를 설명하여라 [5점]

곱셈 암호에서 나쁜 키가 아닌 키들에 대한 역원 <k>는 항상 존재한다.

모듈로-q 의 곱셈에서 q와 서로소인 키 k의 역원 <k>는 항상 존재한다.

따라서 나쁜 키는 30과 1이 아닌 공약수가 존재하는 키이다.

나쁜 키: 2 3 4 5 6 8 9 10 12 14 15 16 18 20 21 22 24 25 26 27 28 30

좋은 키: 1, 7, 11, 13, 17, 19, 23, 29

1. 모듈로가 26이고 블록 크기가 2인 힐 암호에서 키 (k1, k2, k3, k4) = (3,5,6,1) 에 대한 역키 (m1, m2, m3, m4)를 구하고 그 과정을 설명하여라 [5점]

힐 암호의 암호화 공식은 다음과 같음

C1 = k1\*P1 + k2\*P2 mod 26

C2 = k3\*P1 + k4\*P2 mod 26

복호화 하기 위해 두 연립방정식을 풀어야함

이를 위해 첫번째 공식에 k4를, 두번째 공식에 k2를 곱해줌.

k4C1 = k1k4P1 + k2k4P2

ㅡk2C2 = k2k3P1 + k2k4P2

이를 P1과 P2로 정리하면 다음과 같음

P1 = <k1\*k4 - k2\*k3> (k4\*C1 - k2\*C2) mod 26

P2 = <k1\*k4 - k2\*k3> (k1\*C2 - k3 C1) mod 26

이를 간단히 하면 C1, C2의계수들을 다음과 같이 나타낼 수 있음

m1 = <k1\*k4 - k2k3> (k4)

m2 = <k1\*k4 - k2k3> (- k2)

m3 = <k1\*k4 - k2k3> (- k3)

m4 = <k1\*k4 - k2k3> (k1)

k1, k2, k3, k4 = (3, 5, 6, 1)이므로

대입하면

m1, m2, m3, m4 = (25, 5, 6, 23)

[암호화 무작위성]

1. 결정론적 난수 비트 발생기 (deterministic random bit generator) 에 대해서 설명하여라 [5점]

의사난수 비트열 생성을 위해서 PRNG가 실행하는 알고리즘이다.

DRBG는 엔트로피 풀에서 가져온 몇 개의 비트를 그보다 훨씬 긴 비트열로 확장한다.

같은 입력을 넣으면 항상 같은 출력이 나오는 결정론적인 특성을 가지고 있다.

따라서 PRNG는 DRBG에 매번 다른 의사난수 비트열을 생성하기 위해서 같은 입력을 두 번 제공하지 않는다.

1. 무작위성의 실패 사례 중 네스케이프 브라우져의 SSL 구현에서 불충분한 엔트로피원을 얻게 된 이유에 대해서 설명하여라 [5점]

1996년 네스케이프 브라우저의 SSL 구현에서 128 bits PRNG의 종잣값을 계산하는데 에 다음과 같은 의사 코드를 사용했다. 

프로세스 ID와 부모 프로세스 ID 는 각각 15bits 값들이고 b 가 계산되는 항들을 보면 결국 pid, seconds, ppid 는 같은 입력으로 한 번에 들어가게 되므로 ppid 가 12bits 이동되는 것을 고려하여 총 15+12=27bits 가 됨

결과적으로 총 엔트로피가 47 bits 가 되어 128 bits 종잣값에 필요한 128 비트에 미치치 못하게 됨

[암호학적 보안]

1. 암복호화를 위한 키를 보호하는 세 가지 방법에 대해 설명하여라 [5점]
2. 키 포장(key wrapping): 보호할 키를 2차 키로 암호화함

원래의 보호된 키를 복호화하려면

1. 비밀키를 패스워드 로부터 즉석에서 생성한다.

키 포장보다 더 직접적이다.

강도가 약한 패스워드이면 암호화된 메시지의 복호화를 시도해서 정확한 패스워드를 찾는 공격을 수행할 수 있다.

1. 키를 하드웨어 토큰에 저장한다.

키를 패스워드를 입력해야 키를 읽을 수 있는 스마트카드나 USB 장치와 같은 보안메모리에 저장함

컴퓨터가 침해당했을 때도 안전할 수 있음

가장 안전하지만 비용이 가장 비싸고 항상 하드웨어 토큰을 가지고 다녀야 하므로 불편함도 가장 크고 분실할 경우 위험함

[대칭키 암호]

1. 블록 암호에서 슬라이드 공격에 대해서 설명하여라 [5점]
2. 블록 암호에서 전자 코드 북 모드가 비보안성을 지니게 되는 이유를 설명하고, 암호블록 연쇄 모드가 이를 어떠한 방식으로 해결했는 지에 대해서 설명하여라 [5점]

[협업]**<<<<<<<<<실습과제>>>>>>>>>**

실습 과제 부분은 HW1.ipynb 파일을 참고

1. 아핀 암호 [10점]
2. 비즈네르 암호 [20점]
3. 메세지 패딩 [20점]

과제 수행 시에 함께 협업을 했을 경우에는 아래에 협업 내용을 명시. 과제의 어려운 부분을 함께 해결하여 공부하는 것은 가능하지만, 과제 부분을 나누어 작성해서 그대로 복사 하는 것은 0점처리 됨.