암호 응용 및 실습

**HW2**

**제출기한: ~6/17 18:00**

**총점: 80 점 (환산 점수: 20점)**

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

<참고사항>

* 제출 기한이 6/17 18:00 이므로 LMS의 과제 제출 란에 제출 시간전까지 업로드
* 지각 제출: 6/18 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>

* 과제 답변 작성 후에 MS word 파일로 제출

[해시 함수]

1. 해시 함수의 역상 저항성과 충돌 저항성에 대해서 설명하고, 제2 역상 저항성과 충돌 저항성의 차이점에 대해서 설명하여라. [10점]

역상 저항성이란, 어떤 무작위 해시 값이 주어졌을 때 공격자가 그 해시 값의 역상을 찾아낼 수 없다는 보안 보장 속성이다.

역상이란, 주어진 해시 값 H에 대해서 Hash(M) = H 를 만족하는 임의의 메시지 M을 가리켜 그 해시 값의 역상이라고 함

제 1 역상 저항성이란, 주어진 해시 값을 산출하는 메시지를 찾기가 현실적으로 불가능한 것.

제 2 역상 저항성이란, 메시지 M1이 주어졌을 때 그 메시지의 해시 값과 동일한 해시 값을 산출하는 또 다른 메시지 M2를 찾기가 현실적으로 불가능한 것이다.

.

충돌 저항성은 같은 해시 값을 내는 서로 다른 두 메세지를 찾아낼 수 없다는 보안 보장 속성이다.

둘의 차이점은 제 2 역상 저항성은 특정 메시지와 같은 해시를 갖는 다른 메시지를 찾을 수 없다는 보안 보장 속성이고, 충돌 저항성은 아무 메시지가 다른 메시지와 같은 해시 값을 가지는 것을 찾을 수 없다는 보안 보장 속성이다.

1. 해시 함수의 길이 연장 공격에 대해서 설명하여라. [10점]

어떤 미지의 메세지 M이 채움 이후 메세지 블록 M1, M2 로 구성될 때 공격자가 그 메세지의 해시 값 Hash(M)을 안다면 공격자는 임의의 블록 M3에 대한 Hash(M1 ll M2 ll M3) 도 알아낼 수 있는 공격이다.

길이 연장 공격은 해싱된 원래 자료를 모른다고 해도, 또 다른 블록 M3 를 해싱된 메세지에 붙일 수 있기 때문에 가능하다.

해시 함수의 대부분의 응용은 이러한 길이 연장 공격에 영향을 받지 않지만, 해시 함수를 독창적으로 활용할 경우에는 이 문제 때문에 보안이 깨질 수 있다.

이러한 문제는 마지막 암축 함수 실행을 이전의 모든 압축 함수 실행과 조금 다르게 만들면 해결 된다.

[공개키 암호]

1. 공개키 암호 기술의 관점에서 폴리그-헬만 지수 암호에 대해서 설명하여라. (공개키 암호 기술 설명, 암복호화 방법, 공개키 및 복호화 키에 대한 조건 포함). [10점]

공개키 암호 기술은 사전에 비밀키를 공유하거나 비밀 통로를 통해서 키를 직접 공유하지 않고도 안전하게 통신을 할 수 있게 해 주는 방법이다.

폴리그-헬만 지수 암호

가능한 가장 큰 수보다 더 큰 수 중에 소수 p를 선택해야함

키가 되는 암호화 지수 e 는 p-1 과 최대 공약수가 1이어야 됨

(모듈로 p-1에서 곱셈에 대한 역원이 존재하기 위해)

암호화 공식: C=P^e mod p

복호화 공식: P=C^d mod p

모듈로가 소수인 폴리그-헬만 지수 암호의 복호화

페르마의 작은 정리

임의의 소수 p와 p보다 작은 양의 정수 k 에 대해 다음 식이 성립함

k^(p−1) =1 mod p

지수에 대해서는 모듈로 p-1에 대한 연산을 한다고 할 수 있음

C^d = P mod p

P^(ed) = P mod p

P^(p-1) = 1 mod p (페르마의 작은 정리)

ed = 1 mod (p-1)

모듈로가 합성수인 폴리그-헬만 지수 암호의 복호화

오일러 페르마의 정리

임의의 양의 정수 n과 임의의 k 에 대해서 다음 식이 성립함

k^(ϕ(n)) =1 (mod n)

이때, k는 n보다 작거나 같은 양의 정수 중에서 n과 서로소인 수

오일러 파이 함수 (ϕ(n)): n 보다 작거나 같은 양의 정수 중에서 n과 서로소인 수의 개수

지수에 대해서는 모듈로 ϕ(n)에 대한 연산을 한다고 할 수 있음

n이 소수일 경우 페르마의 작은 정리와 동일

소수 p, q, r에 대하여 다음이 성립

ϕ(p) = p-1

ϕ(pq) = pq – p – q + 1

ϕ(pqr) = (p-1)(q-1)(r-1)

오일러 페르마 정리에 의해 다음이 성립

P^(ϕ(n)) = 1= P^0 (mod n)

암호화 지수 e 와 오일러 파이 함수 값 이 서로소일 경우에 복호화 지수를 구할 수 있음

n이 서로 다른 소수의 곱으로 소인수분해 될 경우에는 항상 복호화가 가능함.

그렇지 않으면 P와 n이 서로소여야함

폴리그-헬만 암호의 비밀키 합의

디피-헬먼 키 합의를 통해서 1과 p-1 사이의 수 하나를 비밀키로 얻을 수 있음

g^a mod p, g^b mod p 의 값으로부터 비밀키 g^(ab) mod p 를 알아내는 문제

이를 풀기 위해서는 이산 대수 문제를 풀어야 하지만 이산대수 문제는 효율적으로 풀 수 없음

이산대수 외의 방법으로 푸는 것도 성공하지 못함.

1. RSA 문제가 무엇인지 설명하고, 소인수 분해를 통해서 이를 푸는 방법에 대해서 설명하여라. [10점]

RSA 문제

* + - 1. 아주 큰 소수 두개 (p,q)를 선택함
      2. n = p\*q 에 대해서 ϕ(n) 과 서로소인 e에 대해 d = ( mod ϕ(n) )
      3. n과 e가 공개 암호화 키가 되며, d가 개인 복호화 키가 됨
      4. p, q, ϕ(n) 역시 비밀이지만, 암호화 및 복호화 하는데 필요가 없으므로 버려도 됨

암호화는 공개키를 이용해 C= mod n 진행

복호화는 개인키를 이용해 P= mod n 진행

RSA 보안 수준: n의 크기, p, q 의 선택 등에 달려있음

RSA 문제 해결

방법1: n 소인수분해

지난 오랜 역사에서 소인수분해 문제는 계속해서 다뤄지고 있지만 아직까지 효율적인 해법을 얻지 못함

암호화를 위해서 n을 만들어내는 속도만큼 빨리 n을 소인수분해할 수 없음

방법2: ϕ(n) 계산

ϕ(n)을 알면 d를 계산할 수 n있고, 이로부터 p, q도 구할 수 있으

n과 서로소인 n 미만의 양의 정수 개수를 직접 구함

이러한 문제는 소인수 분해보다도 훨씬 오래 걸림

방법3: d 바로 찾기

복호화 지수 d를 알면, n을 소인수분해할 수 있음

d, e를 알고 있으면 de-1 = 0 (mod ϕ(n))이므로, de-1이 ϕ(n)의 배수이면 됨

사실, ϕ(n)의 배수만 알더라도, n을 소인수분해할 수 있는 확률적 알고리즘이 있음

방법 4: 다음 방정식을 푼다.

C= (mod n)

30년동안 많은 사람이 도전했지만 이것이 가능한지 불가능한지 확실히 밝히지 못함

[기타 공개키 암호]

1. 쓰리-패스 프로토콜에 대해서 설명하고, 쓰리-패스 프로토콜이 작동하기 위한 두 가지 조건에 대해서 설명하여라. [10점]

사전에 만나지 않고도 비밀 메시지를 몰래 전달 할 수 있는 방법 모두 키를 교환하거나 합의해야 함

쓰리 패스 프로토콜은 일반 용도로 쓰기에는 매우 비효율적이지만 비밀키나 키 합의 방식이 필요가 없음

총 3차 패스를 통해서 비밀 메시지를 교환할 수 있음

쓰리 패스 프로토콜이 작동하기 위해서는 다음의 두 가지 속성을 지니 대칭 키 암호가 필요

* + - 1. 밥의 암호화나 앨리스의 암호화가 서로 상대에게 방해가 되어서는 안됨
      2. 앨리스의 암호화와 밥의 암호화 모두 알려진 평문 공격에 저항력이 있어야 함

첫번째 속성을 만족시키기 위해서는 암호화 사이에 교환법칙이 성립해야 함

첫번째 속성과 두번째 속성을 만족시키는 암호는 폴리그-헬만 지수 암호임

1. 머클의 퍼즐에 대해서 설명하고, 머클의 퍼즐이 가지는 한계에 대해서 설명하여라. [10점]

앨리스는 암호화된 메시지(퍼즐)을 만들어 밥에게 보냄

이 때 사용되는 암호화 함수는 무차별 대입 공격을 이용하면 퍼즐이 풀리는 것

128 비트 키를 가진 암호를 사용하되 사용 가능한 키 중에서 극소수만 지정할 것을 제안

퍼즐과 함께 검산용 수를 보냄

검산용 수는 밥이 퍼즐을 맞게 풀었는지 확인하기 위한 검산용으로 모든 퍼즐에 대해 동일함

밥은 퍼즐 하나를 골라 무차별 대입 공격을 통해서 품

검산용 수를 통해서 맞게 풀었는지 확인할 수 있음

해독된 퍼즐의 맨 처음 부분이 암호화된 ID 번호이고 검산용 수 앞까지의 숫자들이 비밀키가 됨

ID 번호를 앨리스에게 보냄

앨리스는 ID 번호로 목록에서 검색하여 비밀키를 알아냄

키 합의 방식

앨리스와 밥은 사전에 직접 만나지 않고도 같은 비밀키를 공유할 수 있음

이브는 밥이 어떤 퍼즐을 선택했는지 모르기 때문에 모든 퍼즐을 다 풀어봐야 함

ID 번호가 주어져도 앨리스가 가진 분류된 퍼즐의 평문 목록이 없음

머클 퍼즐의 한계

앨리스가 퍼즐을 만드는 데에 오랜 시간이 걸리고 저장하려면 많은 공간이 필요

전송하는 데에도 시간이 오래 걸리며 데이터 전송 용량도 매우 커야 함

밥도 무차별 대입 공격으로 퍼즐을 푸는 데 걸리는 시간과 같은 비율로 늘어남

이브에게 필요한 시간이 앨리스와 밥에 비해 훨씬 더 높은 비율로 커지는 키 합의 방식을 개발할 수 있다면 더 실용적으로 사용될 수 있음

1. 타원 곡선 디피-헬만 키 합의에 대해서 설명하여라. (공개키 및 복호화키 설정, 키 합의 과정) [10점]

앨리스와 밥은 공개키 정보인 특정 타원 곡선과 아주 큰 소수 p를 선택함

타원 곡선 암호가 해독이 더 어려울 것으로 추측되기 때문에 모듈로 지수 연산 디피-헬만 체계에서 선택했던 것 보다 상대적으로 작은 소수 p를 선택할 수 있음

앨리스와 밥은 생성자 점 G를 찾음

수 집합에서 모듈로 p에 대한 생성자와는 달리 타원 곡선 위에 있는 모든 점을 생성할 수 있는 점 G를 찾는 일은 불가능함

대신 되도록 많은 점을 생성할 수 있는 점을 찾아야 함

타원 곡선 생성자도 이전처럼 구해져 있는 표에서 찾을 수 있음

공개키: 특정 타원 곡선, 아주 큰 소수 p, 생성자 점 G

키 합의 과정

비밀키로 앨리스는 a, 밥은 b를 고르면 앨리스는 A = aG mod p, 밥은 B = bG mod p 를 서로에게 보냄

앨리스와 밥은 각각 받은 값을 가지고 aB = abG mod p, bA = baG mod p의 값들을 계산하여 비밀키로 사용할 수 있는 비밀 정보를 공유하게 됨

이브가 앨리스와 밥이 공유하는 비밀 정보를 알아내기 위해서는 타원 곡선 디피-헬만 문제를 풀어야 함

aG, bG 로부터 abG 의 값을 알아내야 함

[협업]

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.