HomeWork #2 연습문제

정보보안 이론과 실제

4장

3. 식 (4-3)에서 다음과 같이 RSA 암호화가 제대로 "작동"함을 증명했다.

$$[\{M\}_{앨리스}]_{앨리스} = M$$

다음과 같은 RSA의 서명 확인이 제대로 작동함을 증명하라.

$$\{[M]_{앨리스}\}_{앨리스} = M$$

답변

식 (4-3)은 다음과 같다.

$$C^d = M^{ed} = M^{(ed-1)+1} = M \times M^{ed-1} = M \times M^{k\varnothing(N)} = M \times 1^k = M \bmod N$$

RSA 암호화와 RSA 서명 확인의 차이는 공개키로 암호화하고 개인키로 복호화 하는지 혹은 개인키로 암호화하고 공개키로 복호화 하는지의 차이다. 따라서 다음 식을 만족하므로 식 (4-3)을 사용해 증명할 수 있다.

$$C^d \ (C = M^e \bmod N) = C'^e \ (C' = M^d \bmod N) = M^{ed}$$

4. 앨리스의 RSA 공개키는 $(N,e) = (33,3)$이고 개인키는 $d = 7$이다.

a. 만약 밥이 메시지 $M = 19$를 앨리스를 위해 암호화한다면 암호문 C는 무엇일까? 앨리스가 C를 복호화해 M을 획득할 수 있음을 보여라.

답변

암호문 $C = M^e \bmod N = 19^3 = 6859 = 28 \bmod 33$ 이다. 앨리스는 다음과 같은 식으로 메시지 M을 복호화 할 수 있다.

$$M = C^d \bmod N = 28^7 = 13,492,928,512 = 408,876,621 \times 33 + 19 = 19 \bmod 33$$

b. 앨리스가 메시지 $M = 25$를 전자서명한 결과를 S라고 하자. 이 경우 S는 무엇을 의미할까? 만약 밥이 M과 S를 받았다면, 그 서명을 확인하는 절차를 설명하라. 이 경우에 그 서명이 성공적으로 확인되었음을 보여라.

답변

S는 메시지 $M = 25$을 사용해 앨리스만이 만들 수 있는 서명이다. 만약 밥이 M과 S를 받았다면, 밥은 S를 앨리스의 공개키로 복호화한 다음 그 결과를 M과 비교하면 된다. 복호화한 결과와 M이 같다면 적어도 S를 만든 사람이 앨리스라는 사실은 분명해진다.

13. 앨리스가 밥에게 메시지 M을 전송할 때, 앨리스와 밥은 다음과 같은 프로토콜을 사용한다고 가정하자.

a) 앨리스는 $S=[M]_{앨리스}$를 계산한다.
b) 앨리스는 (M,S)를 밥에게 전송한다.
c) 밥은 $V=\{S\}_{앨리스}$를 계산한다.
d) 만약 $V=M$이면, 밥은 서명이 유효한 것으로 인정한다.

이 프로토콜에서 트루디는 다음과 같은 방법으로 임의 "메시지"에 앨리스의 서명을 위조할 수 있다. 즉, 트루디는 R 값을 생성하고, $N=\{R\}_{앨리스}$를 계산해 (N,R)을 밥에게 전송한다. 위 프로토콜에 따라서 밥은 $V=\{R\}_{앨리스}$를 계산한다. $V=N$이므로 밥은 그 서명을 수용하고 앨리스가 그에게 서명된 아무런 의미가 없는 메시지 N을 보냈다고 믿는다. 결과적으로, 밥은 앨리스를 매우 불쾌하게 생각하게 된다. 이제 다음과 같이 개선된 프로토콜을 가정하자.

a) 앨리스는 $S=[F(M)]_{앨리스}$를 계산한다.
b) 앨리스는 (M,S)를 밥에게 전송한다.
c) 밥은 $V=\{S\}_{앨리스}$를 계산한다.
d) 밥은 $V=F(M)$이면 그 서명을 유효한 것으로 받아들인다.

위에서 언급한 불쾌하게 만든 공격을 방지하기 위해 함수 F가 만족해야 하는 조건은 무엇일까?

답변

역함수가 존재하지 않아야 한다. 역함수가 존재한다면 트루디는 아래와 같은 방법을 써서 밥을 불쾌하게 만들 수 있다. 트루디는 임의 메시지 R을 생성하고 $N=\{R\}_{앨리스}$을 계산해 $(F^{-1}(N),R)$을 밥에게 전송한다. 그러면 밥은 프로토콜에 따라 $V=\{R\}_{앨리스}$를 계산하고 V와 $F(F^{-1}(N))=N$을 비교한다. $V=N$이므로 밥은 그 서명을 수용하게 되고 역시 불쾌하게 생각한다.

22. 다음과 같은 타원곡선 함수가 주어졌다.

$$E: y^2 = x^3 + 7x + b \pmod{11}$$

위 타원곡선과 점 $P = (4,5)$에서 P가 E 선상에 있도록 b를 결정하라. E 선상의 모든 점을 제시하고 E 선상에서 $(4,5) + (5,4)$를 찾아라.

답변

$5^2 = 4^3 + 7 \cdot 4 + b \pmod{11}$ **계산을 해보면** $b = 10$**이다. 그리고 C로 작성한 간단한 연산 프로그램을 통해 구한** E **선상의 모든 점은 (3,5), (3,6), (4,5), (4,6), (5,4), (5,7), (6,2), (6,9),** ∞ **이다. 점(4,5)와 점(5,4)의 기울기** $m = 10$**이고, 정해진 연산을 따르면 두 점의 합은 (3,5)이다.**

23. 다음과 같은 타원곡선을 생각해 보자.

$$E: y^2 = x^3 + 11x + 19 \pmod{167}$$

점 $P = (2,7)$은 E 선 위에 있다. 함수 E와 P가 ECC 디피-헬먼 키교환으로 사용된다고 가정하자. 여기서 앨리스는 비밀 값 $A = 12$, 밥은 비밀값 $B = 31$을 선택했다. 앨리스가 밥에게 전송한 값은 무엇일까? 밥이 앨리스에게 전송한 값은 무엇일까? 공유된 비밀은 무엇일까?

답변

손으로 직접 하기에는 많은 연산을 필요로 하기 때문에 간단한 프로그램을 만들어 답을 구했다. 우선 앨리스는 12*(2,7)을 밥에게 보내고 그 점은 (89, 15)이고, 밥은 앨리스에게 31*(2,7)을 보낸다. 그 점은 (10, 36)이다. 공유된 대칭키는 31*(89, 15) = 12*(10, 36) = (148, 93)이다.

5장

8. 앨리스의 컴퓨터는 대칭키 K_A가 필요하다. 키 K_A를 유도하고 저장하는 다음 두 가지 방법을 생각해 보자.

(i). 그 키는 $K_A = h$(앨리스의패스워드)이며, K_A는 앨리스의 컴퓨터에 저장되어 있지 않다. K_A가 필요할 때마다 앨리스는 패스워드를 입력하여 키를 생산한다.

(ii). 키 K_A는 무작위로 최초 생산되어 $E(K_A, K)$로 저장된다. 여기서 $K = h$(앨리스의패스워드)이다. K_A가 필요할 때마다 앨리스는 그 키를 복호화 하는데 사용하는 패스워드로 들어간다.

(i)번 방법과 (ii)번 방법의 장점을 각각 한 가지씩 들어라.

답변

(i)번 방법의 장점은 키가 컴퓨터에 저장되어 있지 않기 때문에 컴퓨터가 해킹당한다고 해도 키를 안전하게 지킬 수 있다. (ii)번 방법은 키가 컴퓨터에 저장되어 있긴 하지만 암호화 되어 있는 상태이기 때문에 안전하다.

9. 샐리(서버)에 접속하기 위해 사용자 앨리스의 대칭키, 사용자 밥은 다른 대칭키, 사용자 찰리는 또 다른 대칭키가 필요하다고 가정하자. 그래서 샐리는 키 K_A, K_B, K_C를 생성해 이들을 데이터베이스에 저장한다. 다른 방법은 키 다양화 방법이다. 이 방법은 샐리는 하나의 키 K_S를 만들어 저장한다. 이후에 K_A가 요구되면 $K_A = h$(앨리스, K_S)를 만들며 K_B와 K_C도 유사한 방법으로 만들어진다. 키 다양화 방법이 가지는 장점 한 가지와 단점 한 가지를 각각 설명하라.

답변

키 다양화 방법을 사용하면 우선 샐리(서버)측에서 키를 관리하는 것이 편하다. 하지만 만약 K_S가 트루디에게 노출될 경우 모든 사용자의 대칭키가 노출될 가능성이 있다.

12. 밥과 앨리스는 네트워크에서 동전 던지기를 하고자 한다. 앨리스는 다음의 절차를 제안하고 있다.

a) 앨리스가 $X \in \{0,1\}$ 값을 선정한다.
b) 앨리스는 256비트의 무작위 대칭키 K를 만들어낸다.
c) AES를 사용해, 앨리스 $Y = E(X,R,K)$를 계산한다. 여기서 R은 255 무작위 비트이다.
d) 앨리스는 Y를 밥에게 보낸다.
e) 밥은 값 $Z \in \{0,1\}$를 추정해 앨리스에게 말한다.
f) 앨리스는 밥이 $(X,R) = D(Y,K)$를 계산하도록 키 K를 준다.
g) 만약 $X = Z$이면 밥이 이기고, 그렇지 않으면 앨리스가 이긴다.

앨리스가 어떻게 속일 수 있는지를 설명하라. 해시함수를 이용해 앨리스가 속일 수 없도록 이 프로토콜을 수정하라.

답변

앨리스는 임의의 Y를 선정한 후 밥이 복호화 했을 경우 X가 0이 나오는 키와 1이 나오는 키를 따로 만든다. 즉, $(0,R) = D(Y,K_0)$인 K_0와 $(1,R) = D(Y,K_1)$인 K_1를 만든다. 그 다음 밥이 0을 추정하면 K_1을, 1을 추정하면 K_0를 전송한다. 해결 방법은 Y를 생성할 때 만들어낸 K를 해시하여 Y와 같이 전송하면 밥이 X를 추정한 후 K를 앨리스로부터 받아서 해시한 다음 이전에 받았던 해시값과 비교함으로써 앨리스가 속이는 것을 방지할 수 있다.

ps. R의 255비트 전부를 X와 동일하게 설정해서 암호화하면 즉, X가 0이면 0...0(256비트) 1이면 1...1(256)비트를 대칭키 K로 암호화해서 보내는 프로토콜로 수정하면 속임수가 불가능하지 않을까 생각해본다. 다시 말해, R을 고정 비트로 약속한다.
또는 R도 암호문 Y와 함께 전송한다면 위와 같은 속임수는 성사되지 않을 거라 생각한다.