6장 공개키암호

연습문제 풀이

연습문제

1. 키 배송 문제를 해결하는 방법이 아닌 것은?

① 키의 사전 공유에 의한 해결

② 대칭 키 암호에 의한 해결

③ Diffie-Hellman 키 교환

④ 공개 키 암호에 의한 해결

⑤ 키 배포 센터에 의한 해결

연습문제

2. 키 사전 공유에 대한 설명으로 틀린 것은?

① 사전에 사용자 끼리 알고 있는 사람이어야 한다.

② 지리적으로 멀리 있을 경우 사전 공유가 어렵다.

③ 암호 시스템을 이용하는 사용자의 수가 많아지면 사용하기 어렵다.

④ 인터넷이나 우편을 통해 키를 전달하는 것은 위험하다.

⑤ 인편 등을 통해서 직접 전달하는 것이 안전하다.

연습문제

3. Diffie-Hellman 키 교환을 이용하여 암호 통신을 할 경우에 초기에 쌍방이 특정 정보를 서로 교환하는데 이 정보에 대한 설명으로 적합한 것은?

① 이 교환 정보는 사전에 쌍방이 공유하고 있는 값이어야 한다.

② 키 배포 센터에서 제공되는 공통된 값을 교환에 사용한다.

③ 교환된 값을 바로 통신에 키로 사용한다.

④ 도청자가 읽어도 문제가 되지 않는다.

⑤ 대칭 암호 시스템에서 사용하는 대표적인 키 교환 방법이다.

연습문제

4. 공개 키 암호를 이용한 키 배송에 대한 설명으로 적합하지 않은 것은?

① 수신자는 미리 암호화 키를 송신자에게 알려 준다.

② 이 암호화 키는 도청자에게 알려져도 괜찮다.

③ 송신자는 그 암호화 키를 써서 보내고자 하는 메시지를 암호화하고 그것을 수신자에게 보낸다.

④ 수신된 암호문을 복호화할 수 있는 것은 복호화 키를 가지고 있는 사람(수신자)뿐이다.

⑤ 대칭 암호 시스템을 이용한 키 배송이 더 안전하지만 시간이 더 많이 걸리는 단점이 있다.

연습문제

5. 암호 시스템에 대해 올바른 것은?

① 공개 키 암호가 대칭 암호 보다 암호 해독에 더 강하다.

② 공개 키 암호 기술이 보편화 되면 대칭키 암호는 차차로 공개 키 암호로 대체될 것이다.

③ 암호 시스템의 안전도는 키의 길이와 암호 해독에 필요한 계산시간에 좌우된다.

④ 공개 키를 사용하면 키 분배가 대칭키를 사용할 때보다 훨씬 쉬워진다.

⑤ 동일한 키의 길이라면 공개 키 암호가 더 안전하다.

연습문제

6. 공개 키 암호에 대한 설명으로 적합하지 않는 것은?

① 암호화 키와 복호화 키 모두 비밀로 해야 한다.

② 송신자가 필요한 것은 암호화 키뿐이다.

③ 수신자가 필요한 것은 복호화 키뿐이다.

④ 도청자에게 알려지면 곤란한 것은 복호화 키이다.

⑤ 암호화 키는 도청자에게 알려져도 괜찮다.

연습문제

7. 공개 키 암호구조의 핵심요소가 아닌 것은?

① 평문과 암호문

② 암호 알고리즘

③ 공개 키와 개인 키

④ 복호 알고리즘

⑤ 인증서

연습문제

8. 공개 키를 이용하면 암호의 키 배송 문제를 해결 할 수 있다. 하지만 이것으로 모든 문제가 없어진 것은 아니다. 입수한 공개 키가 정말로 바른 공개 키인지 어떤지를 판단할 필요가 있기 때문이다. 그 이유로 다음의 어떤 공격이 가능하기 때문인가?

① 전수 공격　② 생일 공격　③ 중간자 공격

④ 서비스 거부 공격　⑤ 재전송 공격

연습문제

9. RSA 암호 시스템의 안전성을 보장해주는 것으로 적합하지 않은 것은?

① 현재는 2048비트 이상의 키를 사용하면 현실적으로 해독이 어렵다.

② 공개 키를 알고 있다고 해도 개인 키를 알 수 있는 방법이 없다.

③ 공개 키의 N 값을 소인수 분해하는 데 시간이 많이 걸린다.

④ 이산 대수를 구하는 빠른 방법을 알지 못하기 때문이다.

⑤ 큰 소수가 부족하기 때문이다.

연습문제

10. 다음 중 공개 키 방식 암호 알고리즘이 아닌 것은?

① ElGamal 방식

② Rabin 방식

③ Diffie-Hellman 방식

④ Rijndael 방식

⑤ ECC 방식

참고문헌

- 암호학과 네트워크 보안, Behrouz A. Forouzan 지음, 이재광외 3인 역, 한티미디어
- 컴퓨터 보안과 암호, WILLIAM STALLINGS 지음, 최용락외 2인 역, 그린출판사
- 암호 알고리즘 및 키길이 이용 안내서, KISA-GD-2018-0034, 한국인터넷진흥원
- 금융부분 암호기술 활용 가이드, 금융보안원, 2019.1