2017-2 5차 과제물 제출기한: 2017년 12월 20일(수)까지	현대암호 이론 및 응용	학번	
		성명	

※다음 문장의 내용이 맞으면 ○표, 틀리면 ×표를 답하시오.

1. 디지털서명은 메시지 인증이나 메시지 무결성은 보장할 수 있지만, 메시지 기밀성을 보장하지 못한다.
2. 데이터 근원에 대한 메시지 인증과 주장자의 신원을 확인하기 위한 개체 인증 둘 다 모든 메시지에 대해 반복적으로 인증 과정을 수행해야만 한다.
3. 일회용 패스워드(one-time password)는 한번만 사용되므로 도청이나 도난이 발생하더라도 안전에 문제가 없다.
4. 디지털 서명을 이용하면 메시지 인증을 할 수 있다. 또한 메시지 자체에 서명을 하는 대신에 메시지 다이제스트에 서명을 하게 되면 메시지 무결성은 물론 서명 자체에 대한 부인 봉쇄도 가능하다.
5. 시도-응답 인증(challenge-response authentication)이 성공적으로 이루어지기 위해서는 주장자가 검증자에게 자신의 비밀을 제3자에게 노출되지 않도록 안전한 방법으로 보내 자신이 비밀을 알고 있다는 사실을 증명하여야 한다.
6. 영지식 인증에서 주장자는 자신의 비밀을 노출하지 않는다. 그럼에도 불구하고 주장자는 자신이 그 비밀을 알고 있다는 사실만을 증명할 수 있어야 한다.
7. 커버로스(Kerberos)는 인증 프로토콜인 동시에 자체적으로 키-배분센터(KDC)의 역할을 수행한다.
8. 디지털 서명은 문서와 분리된 별도의 파일 형태로 보내질 수 있으므로, 서명이 재사용되지 못하도록 공개된 해쉬함수를 이용해 만들어진 메시지 다이제스트에 서명을 하여야 한다.
9. Diffie-Hellman 프로토콜을 이용하면 키-배분센터(KDC)를 거치지 않고 당사자 간에 세션에 사용될 대칭 키를 직접 만들어 사용할 수 있다.
10. Diffie-Hellman 프로토콜에서 군과 생성자에 관한 정보, 즉 p와 g의 값은 인터넷을 통해 서로 주고받는 과정에서 공개되더라도 세션에 사용될 대칭 키의 안정성에는 영향을 주지 않아야 한다.

1	2	3	4	5	6	7	8	9	10

※ 다음 괄호에 알맞은 값이나 용어를 채워 넣으시오.

11. 특정 사람에 대한 개체 인증을 위해 사용되는 것을 크게 3가지로 나누어 분류하면 알고 있는 것(something known), 소유하고 있는 것(something possessed), ( )으로 구분된다.
12. ( ) 디지털 서명 구조는 문서의 내용을 서명자에게 보여주지 않으면서 서명을 하도록 만들 수 있다.
13. 커버로스(Kerberos) 프로토콜에서는 사용자에게 서비스를 제공하는 실질 서버이외에 키-분배센터(KDC)를 구성하는 ( ) 서버와 ( ) 서버를 사용한다.
14. 인증서 폐기 목록(CRL)의 업데이트 주기 사이에 변경이 생길 경우, 가장 최근에 업데이트된 최신 목록 이후에 변경사항만 기록된 것을 ( ) 인증서 폐기 목록이라고 부른다.
15. 생체인식기술의 정확도를 측정하기 위한 매개변수의 하나인 ( )은 인식되어야 할 사람이 얼마나 자주 시스템에 의해서 인식이 되지 않은 지를 나타낸다.

11	
12	
13	
14	
15	