2018-서울시-정보보호론-A형-해설-곽후근

1. 2009년 Moxie Marlinspike가 제안한 공격 방식이며, 중간자 공격을 통해 사용자와 서버 사이의 HTTPS 통신을 HTTP로 변경해서 비밀번호 등을 탈취하는 공격 방식으로 가장 옳은 것은?
① SSL stripping
② BEAST attack
③ CRIME attack
④ Heartbleed
정답 체크 :
(1) SSL stripping : 공격자가 중간에서 SSL로 보호되는 세션을 벗겨내는 것이다. 즉, 공격자는 MITM(중간자) 상태를 클라이언트-공격자-웹서버로 만들어서 클라이언트와 공격자 사이에서는 HTTP로 통신되게끔 유도하고 공격자와 웹서버에서는 HTTPS(SSL)로 통신한다.
오답 체크 :
(2) BEAST attack : SSL 통신에서 브라우저가 가지는 취약점이다. 해당 공격은 CBC(블록암호 모드의 일종)의 취약점을 이용한다. CBC 취약점을 이용하면 SSL 상에서 MITM 공격(중간자 공격)이 가능하다.
(3) CRIME attack : HTTPS를 사용한 연결에서 웹 쿠키의 보안 취약점이다. 인증 쿠키의 내용을 알게 되면 공격자는 웹 세션에서 세션 하이재킹을 수행할 수 있다.
(4) Heartbleed : 암호 통신 라이브러리 OpenSSL(SSL의 오픈 소스 구현판)의 버그이다. 공격자는 이 취약성을 내포한 OpenSSL을 사용하고 있는 서버에 접속하여 서버의 정보를 일정 범위까지 갈취 가능하다.

2. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?
① 게시판 등의 웹페이지에 악의적인 코드 삽입이 가능하다는 취약점이 있다.
② 공격 코드를 삽입하는 부분에 따라 저장 XSS 방식과 반사 XSS 방식이 있다.
③ 악성코드가 실행되면서 서버의 정보를 유출하게 된다.
④ Javascript, VBScript, HTML 등이 사용될 수 있다.
정답 체크 :
(3) 악성코드가 실행되면서 클라이언트(사용자)의 정보(쿠키)를 유출한다.
오답 체크 :
(1) 저장 XSS(접속자가 많은 웹 사이트를 대상으로 공격자가 XSS 취약점이 있는 웹 서버에 공격용 스크립트(script)를 입력시켜 놓으면, 방문자가 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격하는 방식) 공격에 해당한다.
(2) 저장 XSS, 반사 XSS(악성 스크립트가 포함된 URL을 사용자가 클릭하도록 유도하여 URL을 클릭하면 URL을 반사하여 URL에 포함된 악성 스크립트를 클라이언트에서 실행), DOM 기반 XSS 공격(DOM(Document Object Model) 환경에서 악성 URL을 통해 사용자의 브라우저를 공격, 서버에 반사되지 않고 클라이언트에서 실행) 방식이 있다.
(4) Client-side scripting(클라이언트에서 악성 스크립트가 실행됨)인 Javascript, VBScript, HTML 등이 사용될 수 있다.

3. 〈보기〉에서 설명하는 보안 목적으로 가장 옳은 것은?

〈보기〉 정보가 허가되지 않은 방식으로 바뀌지 않는 성질

① 무결성(Integrity)
② 가용성(Availability)
③ 인가(Authorization)
④ 기밀성(Confidentiality)

정답 체크 :

(1) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.

오답 체크 :

(2) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.

(3) 인가 : 인증은 사용자의 신원을 증명하는 것이고, 인가는 특정 리소스에 접근할 수 있는 권한을 부여한 것이다.

(4) 기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.

4. 「개인정보 보호법」 상 용어 정의로 가장 옳지 않은 것은?

① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록 번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
② 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
④ 개인정보관리자: 업무를 목적으로 개인정보파일을 운용 하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

정답 체크 :

(4) “개인정보 보호법” 제2조(정의) 상 해당 설명은 개인정보처리자를 의미한다. “정보통신망법” 제27조(개인정보 관리책임자의 지정) 상 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

5. Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

정답 체크 :

(3) SPN 암호 방식을 사용한다.

오답 체크 :

(1) 평문 블록의 길이는 최소 128비트이고, 키의 길이는 최소 128비트이고, 라운드 수는 16라운드 이상으로 해야한다.
(2) 암호화와 복호화 과정은 동일하다.
(4) 대칭키 암호인 DES, Blowfish, SEED 등에서 사용한다.

6. 디지털 서명에 대한 설명으로 옳은 것을 〈보기〉에서 모두 고른 것은?

〈보기〉 ㄱ. 디지털 서명은 부인방지를 위해 사용할 수 있다. ㄴ. 디지털 서명 생성에는 개인키를 사용하고 디지털 서명 검증에는 공개키를 사용한다. ㄷ. 해시 함수와 공개키 암호를 사용하여 생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ
정답 체크 :
(1)
(ㄱ) : 디지털 서명은 개인키로 암호화(서명)를 수행하기 때문에 자신이 서명한 것에 대해서 부인할 수 없다.
(ㄴ) : 디지털 서명은 개인키 암호화(개인키로 암호화(서명), 공개키로 복호화(검증))이다. 즉, 공개키 암호화(공개키로 암호화, 개인키로 복호화)의 반대이다.
오답 체크 :
(2), (3), (4)
(ㄷ) : 디지털 서명은 인증, 무결성, 부인방지를 제공한다. 기밀성을 제공하기 위해서는 별도의 암호화를 수행하여야 한다.

7. 분산반사 서비스 거부(DRDoS) 공격의 특징으로 가장 옳지 않은 것은?
① TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한다.
② 공격자의 추적이 매우 어려운 공격이다.
③ 악성 봇의 감염을 통한 공격이다.
④ 출발지 IP 주소를 위조하는 공격이다.
정답 체크 :
(3) 해당 설명은 DDoS에 대한 설명이다.
오답 체크 :
(1) TCP 3-way handshake의 취약점과 반사 서버(라우터 등)를 이용한다.
(2) 출발지 IP를 공격 대상의 IP로 위조하므로 공격자의 추적이 어렵다.
(4) 출발지 IP를 공격 대상의 IP로 위조한다.

8. 침입탐지시스템의 비정상행위 탐지 방법에 대한 설명으로 가장 옳지 않은 것은?
① 정상적인 행동을 기준으로 하여 여기서 벗어나는 것을 비정상으로 판단한다.
② 정량적인 분석, 통계적인 분석 등을 사용한다.

③ 오탐률이 높으며 수집된 다양한 정보를 분석하는 데 많은 학습 시간이 소요된다.
④ 알려진 공격에 대한 정보 수집이 어려우며, 새로운 취약성 정보를 패턴화하여 지식데이터베이스로 유지 및 관리하기가 쉽지 않다.
정답 체크 :
(4) 해당 설명은 비정상행위(anomaly)가 아니라 오용(misuse) 탐지에 해당 설명이다.
오답 체크 :
(1) 비정상적인 패킷을 차단하다. 예를 들어, 초당 100개의 syn 패킷을 받기로 설정하면 초과하는 패킷은 비정상 패킷이므로 해당 패킷은 버린다.
(2) 통계적 접근(과거의 통계 자료를 바탕으로 사용자의 행위를 관찰하여 프로파일을 작성하고 프로파일과 사용자 행위의 비교를 통해 비정상 정도를 측정), 예측 가능 패턴 생성(현재까지 발생한 사건들을 바탕으로 다음 사건을 예측), 신경망 방식(신경망을 이용하여 현재까지의 사용자의 행동이나 명령이 주어졌을 때 다음 행동이나 명령을 예측) 등이 존재한다.
(3) 비정상적인 패킷을 차단하므로 정상적인 패킷도 차단할 확률이 존재한다. 비정상적인 패킷을 차단하기 위해 분석을 하는데 수집된 데이터의 양이 많으므로 많은 학습 시간이 소요된다.

9. 메모리 변조 공격을 방지하기 위한 기술 중 하나로, 프로세스의 중요 데이터 영역의 주소를 임의로 재배치하여 공격자가 공격 대상 주소를 예측하기 어렵게 하는 방식으로 가장 옳은 것은?
① canary
② ASLR
③ no-execute
④ Buffer overflow
정답 체크 :
(2) ASLR : 메모리 공격을 방어하기 위해 주소 공간배치를 난수화하는 기법이다.
오답 체크 :
(1) canary : 컴파일러가 프로그램의 함수 호출 시에 복귀 주소 앞에 canary(밀고자, Random, NULL, Terminator(CR, LF)) 값을 주입하고, 종료 시에 canary 값 변조 여부 확인한다.
(3) no-execute : 스택에서 프로그램(eggshell-공격자의 쉘 코드)을 실행할 수 없게 한다.
(4) Buffer overflow : 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다.

10. 퍼징(fuzzing)에 대한 설명으로 가장 옳은 것은?
① 사용자를 속여서 사용자의 비밀정보를 획득하는 방법이다.
② 실행코드를 난독화하여 안전하게 보호하는 방법이다.
③ 소프트웨어 테스팅 방법 중 하나로 난수를 발생시켜서 대상 시스템에 대한 결함이 발생하는 입력을 주입하는 방법이다.
④ 소스 코드를 분석하는 정적 분석 방법이다.
정답 체크 :
(3) 컴퓨터 프로그램에 유효한, 예상치 않은 또는 무작위 데이터를 입력하는 것이다. 이후 프로그램은 충돌이나 잠재적인 메모리 누수 발견 등 같은 예외에 대한 감시가 이루어진다.
오답 체크 :
(1) 사회공학 기법을 의미한다.

(2) goto 문 등을 이용해서 코드를 리버스 엔지니어링(실행코드에서 소스코드를 얻어냄)할 수 없게 하는 것이다.
(4) 정적 분석은 소스 코드를 분석하는 것이고, 동적 분석은 실행 과정을 분석하는 것이다.

11. 보안 측면에서 민감한 암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고자 나온 개념으로, TCG 컨소시엄에 의해 작성된 표준은?
① TPM
② TLS
③ TTP
④ TGT
정답 체크 :
(1) TPM(Trusted Platform Module) : 국제산업표준단체인 TCG(Trusted Computing Group)에 의해 작성된 암호화 키 관리와 암호화 처리 등을 하드웨어로 제조된 보안 칩 내부에서만 동작하도록 함으로써 강력한 수준의 보안 환경을 제공하는 보안 칩의 표준 규격이다.
오답 체크 :
(2) TLS(Transport Layer Security) : Https에 사용하는 SSL/TLS(4계층에서 보안 제공)를 나타낸다.
(3) TTP(Trsuted Third Party) : 믿을 수 있는 제3자로 PKI(공개키 기반 구조)에서 CA(인증 기관)을 나타낸다.
(4) TGT(Ticket Granting Ticket) : Kerberos에서 사용하는 티켓으로 클라이언트가 AS(인증서버)로부터 받아 TGS(티켓 발행 서버)로 보낸다(서버에 사용할 티켓을 제공받기 위해).

12. 사회 공학적 공격 방법에 해당하지 않는 것은?
① 피싱
② 파밍
③ 스미싱
④ 생일 공격
정답 체크 :
(4) 생일 공격 : 어떤 모임에서 사람이 수가 증가할수록 생일이 같을 확률이 증가함을 의미한다. 예를 들어, 해시의 입력값을 증가하면 같은 출력값을 가지는 입력값을 가지는 확률이 증가하게 된다.
오답 체크 :
(1) 피싱 : Private data(개인 정보)와 fishing(낚는다)의 합성어이다. 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보와 같은 개인정보를 빼내는 사기기법을 말한다.
(2) 파밍 : Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다. 해당 공격 기법을 이용하여 공격자의 웹서버 IP 주소와 정상 사이트의 도메인 주소를 매핑해 준다.
(3) 스미싱 : SMS(문자 메시지)와 Phishing의 약자이다. Phishing은 Private Data(개인 정보)와 Fishing(낚시)의 약자이다. 공격자가 문자 메시지에 URL을 보내고, 사용자가 이를 클릭하면 해킹 툴이 스마트폰에 설치되어 개인 정보가 탈취된다.

Tip! : 사회 공학적 공격이란 인간의 마음을 교묘하게 이용하는 공격기법으로 생일 공격은 이에 해당하지 않는다.

13. 접근 제어 방식 중, 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용되는 방식은?
① 접근 제어 행렬(Access Control Matrix)
② 접근 가능 목록(Capability List)
③ 접근 제어 목록(Access Control List)
④ 방화벽(Firewall)
정답 체크 :
(2) 접근 가능 목록(Capability List) : 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용한다. ACL과 다른 점은 권한 위임이 가능하다(transferable).
오답 체크 :
(1) 접근 제어 행렬(Access Control Matrix, ACM) : 주체와 객체 쌍에 대해 어떤 권한이 부여되었는지를 나타낸다.
(3) 접근 제어 목록(Access Control List, ACL) : 주체의 관점에서 객체들에 대한 권한을 다루거나 객체의 관점에서 주체들의 권한을 다룬다.
(4) 방화벽(Firewall) : 방화벽에서는 ACL을 사용한다.

14. WPA2를 공격하기 위한 방식으로, WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격 방식으로 가장 옳은 것은?
① KRACK
② Ping of Death
③ Smurf
④ Slowloris
정답 체크 :
(1) KRACK : Key Reinstallation Attack으로 치명적인 재전송 공격이다. WPA2 핸드쉐이크의 3단계에서 전송되는 난수를 반복적으로 리셋을 수행하여 암호화된 패킷을 매칭해 봄으로써 암호화에 사용했던 키를 알아낼 수 있다.
오답 체크 :
(2) Ping of Death : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(3) Smurf : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
(4) Slowloris : 최소 대역폭과 사용하지 않는 서비스와 포드를 이용해서 서버에 많은 연결을 맺고 최대한 길게 연결을 지속한다. 주기적으로 HTTP 요청을 하고 요청을 멈추거나 끝내지 않는다.

15. 오일러 함수 $\phi(\ )$를 이용해 정수 n=15에 대한 $\phi(n)$을 구한 값으로 옳은 것은? (단, 여기서 오일러 함수 $\phi(\ )$는 RSA 암호 알고리즘에 사용되는 함수이다.)

① 1
② 5
③ 8
④ 14

정답 체크 :

(3)

오일러 피 함수(Euler's phi(totient) function) $\phi(n)$는 n이 양의 정수일 때, n과 서로소인 1부터 n까지의 정수의 개수와 같다. 즉, 오일러 피 함수는 1부터 14까지 15와 서로소의 개수를 묻는 질문이다. 1부터 14까지 15와 서로소((1, 2, 4, 7, 8, 11, 13, 14)는 8개이다. 여기서 서로소(coprime)는 공약수(동시에 그들 모두의 약수(어떤 수가 정수로 나누어떨어지는 것)인 정수)가 1뿐인 두 정수를 의미한다. 예를 들어, 8과 15는 공약수가 1이므로 서로소이다.

16. 능동적 공격으로 가장 옳지 않은 것은?

① 재전송
② 트래픽 분석
③ 신분위장
④ 메시지 변조

정답 체크 :

(2) 트래픽 분석 : 기밀성을 해치는 수동적(소극적) 공격이다.

오답 체크 :

(1) 재전송 : 무결성을 해치는 능동적(적극적) 공격이다.
(3) 신분위장 : 무결성을 해치는 능동적 공격이다.
(4) 메시지 변조 : 무결성을 해치는 능동적 공격이다.

17. 무선랜 보안에 대한 설명으로 옳은 것을 〈보기〉에서 모두 고른 것은?

〈보기〉
ㄱ. WEP는 RC4 암호 알고리즘을 사용한다.
ㄴ. WPA는 AES 암호 알고리즘을 사용한다.
ㄷ. WPA2는 EAP 인증 프로토콜을 사용한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 체크 :

(2)

(ㄱ) : WEP는 RC4 암호 알고리즘을 사용한다.
(ㄷ) : WPA2는 802.1x에서 EAP 인증 프로토콜을 사용한다.

오답 체크 :

(1), (3), (4)
(ㄴ) : WPA는 RC4 암호 알고리즘을 사용하고, WPA2가 AES 암호 알고리즘을 사용한다.

18. BLP(Bell & La Padula) 모델에 대한 설명으로 가장 옳지 않은 것은?
① 다단계 등급 보안(Multi Level Security) 정책에 근간을 둔 모델이다.
② 기밀성을 강조한 모델이다.
③ 수학적 모델이다.
④ 상업용 보안구조 요구사항을 충족하는 범용 모델이다.
정답 체크 :
(4) BLP, Biba는 상업용 관점이 아니고, Clark-Wilson, Chinese-Wall이 상업용 관점이다.
오답 체크 :
(1) 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지한다. 즉, 다단계 보안 레벨을 가진다.
(2) 미 국방부 지원 보안 모델로 보안 요소 중 기밀성 강조한다.
(3) 최초의 수학적 모델로 강제적 정책에 의해 접근 통제하는 모델이다.

19. 〈보기〉와 관련된 데이터베이스 보안 요구 사항으로 가장 옳은 것은?

〈보기〉 서로 다른 트랜잭션이 동일한 데이터 항목에 동시적으로 접근하여도 데이터의 일관성이 손상되지 않도록 하기 위해서는 로킹(locking) 기법 등과 같은 병행 수행 제어 기법 등이 사용 되어야 한다.

① 데이터 기밀성
② 추론 방지
③ 의미적 무결성
④ 운영적 무결성
정답 체크 :
(4) 운영적 무결성 : 트랜잭션의 벼행 처리 동안에 데이터에 대한 논리적 일관성을 보장해야 한다.
오답 체크 :
(1) 데이터 기밀성 : 중요 데이터에 대한 기밀성을 보호하고 인가된 사용자에 대해서만 접근을 허용해야 한다.
(2) 추론 방지 : 사용자가 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적(추론)할 수 없어야 한다.
(3) 의미적 무결성 : 데이터에 대한 허용 값을 통제함으로써 변경 데이터의 논리적 일관성을 보장해야 한다.
Tip! : 데이터베이스의 보안 요구 사항을 테이블로 정리하면 다음과 같다.

보안 요구사항	내용
부적절한 접근 방지	승인된 사용자에게만 접근 권한을 부여하고, 사용자나 응용시스템의 접근 요청에 대해 정당성 여부를 검사해야 한다.
추론 방지	사용자가 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적(추론)할 수 없어야 한다.
무결성 보장	인가되지 않은 접근, 저장 데이터를 손상시킬 수 있는 시스템 오류, 고장,

	파업 등으로부터 데이터베이스를 보호해야 한다.
운영적 무결성 보장	트랜잭션의 벼행 처리 동안에 데이터에 대한 논리적 일관성을 보장해야 한다.
의미적 무결성 보장	데이터에 대한 허용 값을 통제함으로써 변경 데이터의 논리적 일관성을 보장해야 한다.
감사 기능	데이터베이스에 대한 모든 접근이 감사 기록(로그)을 생성해야 한다.
사용자 인증	운영체제에서 수행하는 사용자 인증보다 엄격한 인증이 필요하다.
기밀성 보장	중요 데이터에 대한 기밀성을 보호하고 인가된 사용자에 대해서만 접근을 허용해야 한다.

20. RSA에 대한 설명으로 가장 옳지 않은 것은?

① AES에 비하여 암, 복호화 속도가 느리다.

② 키 길이가 길어지면 암호화 및 복호화 속도도 느려진다.

③ 키 생성에 사용되는 서로 다른 두 소수(p, q)의 길이가 길어질수록 개인키의 안전성은 향상된다.

④ 중간자(man-in-the-middle) 공격으로부터 안전하기 위해서는 2,048비트 이상의 공개키를 사용하면 된다.

정답 체크 :

(4) 일단 중간자 공격은 공개키 길이와 무관하다. 그러므로 공개키 길이를 늘려도 중간자 공격을 막을 수 없다.

오답 체크 :

(1) AES(대칭키, 치환과 순열을 이용)와 다르게 RSA(공개키)는 수학적 계산에 암호화/복호화를 수행하므로 속도가 더 느리다.

(2) 키 길이가 길어지면 수학적 계산량이 증가하여 암호화/복호화 속도가 느려진다.

(3) p와 q의 곱으로 만들어지는 N은 공개되는데, 공개되는 N은 소인수분해 공격이 가능하다. 그러므로 p와 q의 길이를 길게하면 소인수분해 공격으로부터 안전하다.