

정보보호기술

2017년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :                      성명 :

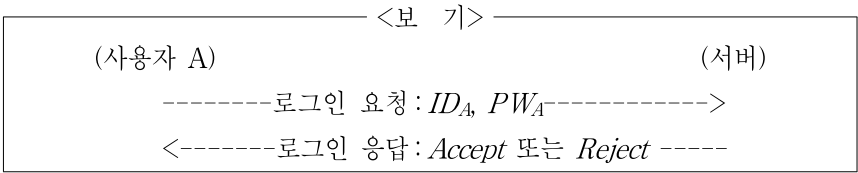
제 1 문. 암호학적 해시 함수(Cryptographic Hash Function)는 해시 함수의 일종으로 역상 저항성(Pre-image Resistance), 2차 역상 저항성(Second Pre-image Resistance), 그리고 충돌 저항성(Collision Resistance)의 성질을 갖고 있어야 한다. 암호학적 해시 함수에 대해 다음의 물음에 답하시오. (총 20점)

- 1) 역상 저항성, 2차 역상 저항성, 충돌 저항성의 개념을 설명하시오. (6점)
- 2) SHA(Secure Hash Algorithm)-512는 512비트 해시값을 생성하는 암호학적 해시 함수이다. SHA-512를 이용하여 2600비트 메시지의 해시값을 구하고자 할 때, 메시지에 추가되어야 할 패딩 비트는 몇 비트인지 계산하시오. (6점)
- 3) SHA-512의 안전성을 생일 역설(Birthday Paradox)의 관점에서 설명하시오. (8점)

제 2 문. 다음은 고전 암호에 관한 문제이다. 알파벳 집합  $Z = \{a, b, c, \dots, z\}$ 라고 할 때 물음에 답하시오. (총 15점)

- 1) 줄리어스 시저(Caesar)가 사용했던 시저 암호는 평문으로 사용되는 알파벳을 일정한 문자 수 만큼 평행이동시킴으로써 암호화를 행한다. 시저 암호가 전사 공격(Brute-force Attack)에 취약한 이유를 설명하시오. (5점)
- 2) 임의의 일대일 대응 함수  $f : Z \rightarrow Z$ 를 사용하는 단일치환암호(단일문자암호, Monoalphabetic Cipher)의 전사 공격에 대한 안전성을 설명하시오. (5점)
- 3) 2)에서 언급한 단일치환암호의 통계적 공격(빈도분석 공격, Statistical Attack)에 대한 안전성을 설명하시오. (5점)

제 3 문. 네트워크에 연결된 사용자 A가 서버 접속에 필요한 아이디  $ID_A$ 와 패스워드  $PW_A$ 를 가지고 원격 서버에 로그인 한다고 하자. 다음 물음에 답하시오. (총 15점)



- 1) <보기>와 같은 방식으로 서버가 사용자의 로그인 요청을 승인( $Accept$ ) 또는 거부( $Reject$ )하도록 로그인 프로토콜을 구성할 때, 이 프로토콜의 취약점을 설명하시오. (7점)
- 2) <보기>의 프로토콜의 취약점을 개선하고 로그인 횟수를 최대  $n$ 번으로 제한하고자 할 때, Leslie Lamport가 제안한 해시체인(Hash Chain)을 이용한 일회용 패스워드를 사용하여 로그인 프로토콜을 설계하시오. (8점)

인사혁신처 시험출제과장