

컴퓨터네트워크

2012년 시행 5급(기술) 공채 제2차시험

응시번호 :

성명 :

제 1 문. TCP(Transmission Control Protocol)에 대한 다음 물음에 답하시오. (총 15점)

- 1) TCP 전송 속도 제어의 목표는 크게 링크 사용율의 최대화, 혼잡 상황의 해소, 타 트래픽과의 공평성 확보이다. 이 중 타 트래픽과의 공평성 확보를 위해 TCP에서 사용하는 방법을 설명하시오. (5점)
- 2) TCP는 네트워크 혼잡 상황을 예측하기 위해 타임아웃(Time-out)과, Triple Duplicative Acknowledgement의 수신, ECN(Explicit Congestion Notification)의 수신을 사용한다. 이들 세 가지 방식을 사용할 때, 혼잡 상황 예측에 소요되는 시간을 비교하시오. (5점)
- 3) 인터넷 라우터에서 흔히 사용하는 큐 관리 기법인 Drop Tail 방식은 라우터의 큐에 더 이상의 자리가 없을 때, 새로 도착하는 패킷을 폐기한다. 이러한 Drop Tail 방식은 구현의 간단함으로 인해 인터넷에서 널리 사용되고 있으나, TCP의 성능을 저하시킬 수 있다고 알려져 있다. 이러한 문제를 해결하고자 제안된 RED(Random Early Detection) 기법은 라우터의 큐에 저장된 패킷의 수가 일정 수 이상으로 증가할 때, 정해진 확률로 패킷을 폐기한다. Drop Tail 방식이 TCP의 성능을 저하시킬 수 있는 주요 원인을 설명하고, RED 방식이 이를 어떻게 해결할 수 있는지 설명하시오. (5점)

제 2 문. 다음과 같은 조건을 갖는 무선 LAN에 대한 다음 물음에 답하시오. (총 15점)

- 무선 스테이션(wireless station)은 802.11 b 무선 랜 표준(데이터 전송률 a bps)으로 동작한다.

○ 전파 지연은 없으며 BER(Bit Error Rate)은 0이다.

○ 제어 프레임(RTS, CTS, ACK)의 크기는 모두 동일하며, 전송에 소요되는 시간은 모두 t로 동일하다.

- 1) RTS/CTS를 사용하는 CSMA/CA 프로토콜에서 임의의 출발지 무선 스테이션이 목적지 무선 스테이션으로 β bits 크기의 데이터 프레임 전송을 완료(ACK 수신 포함)할 때까지 걸리는 최소 전송 시간을 DIFS 및 SIFS, t, a, β 의 함수로 나타내시오. (단, 다른 스테이션들은 모두 유힘(idle) 상태에 머물러 있다고 가정한다) (5점)
- 2) 1)에서 송신기의 전송범위에 위치하지 않고 수신기의 전송범위에 위치한 은닉 스테이션(Hidden Terminal)이 수신한 NAV(Network Allocation Vector) 값을 계산하시오. (5점)
- 3) CSMA/CA의 RTS/CTS 메시지 교환 방식이 드러난 스테이션(Exposed Terminal) 문제를 해결하지 못하는 이유를 설명하시오. (5점)

제 3 문. 컴퓨터 보안분야에서 encryption과 decryption key를 안전하게 교환하는 것이 중요한 문제이다. 이러한 문제를 해결하기 위해 두 가지 방식이 제안되었다. 즉, secret key를 배분하기 위해서는 Diffie-Hellman 방식을, public key를 배분하기 위해서는 RSA 알고리즘과 X.509 프로토콜을 사용한다. 다음 물음에 답하시오. (총 20점)

- 1) Diffie-Hellman 방식에서는 Alice와 Bob이 random number인 x 와 y 를 각각 선택하고 Alice는 $(n, g, g^x \bmod n)$ 을, Bob은 $(g^y \bmod n)$ 을 상대방에게 전송한다. 이 때 g 와 n 은 Alice와 Bob이 이미 알고 있는 큰 숫자로 특정조건을 만족한다. 이러한 두 개의 메시지를 교환한 후에 Alice와 Bob이 갖는 secret key를 계산하시오. 또한 plain text로 기술된 이들 두 개의 메시지를 보고도 Alice가 계산한 secret key를 제 3자인 Trudy가 알아내기 어려운 이유를 설명하시오. (5점)
- 2) RSA 알고리즘은 두 개의 소수(prime number) p 와 q 를 선택하여, $n = p*q$, $z = (p-1)*(q-1)$ 을 계산하고, z 에 대해 소수인 d 와 $e*d = 1 \bmod z$ 를 만족하는 e 를 각각 계산한다. 이 때 (e, n) 은 public key로, (d, n) 은 private key로 사용하게 된다. $p = 3$ 과 $q = 11$ 일 때, 가능한 한 개의 public key와 private key를 계산하시오. 또한 public key (e, n) 을 알고도 private key (d, n) 을 계산하기 어려운 이유를 설명하시오. (5점)

- 3) RSA 알고리즘에서 encryption과 decryption 방식은 $m^e \bmod n = c$ 를 이용한다. 이 때 m 은 plain text이고 c 는 cipher text를 의미한다. 다음의 정리를 이용하여 RSA알고리즘을 이용했을 때, $c^d \bmod n = m$ 이 성립됨을 증명하시오. (5점)

$$p \text{와 } q \text{가 소수이고 } n = p*q \text{이면, } x^y \bmod n = x^{(y \bmod (p-1)*(q-1))} \bmod n$$

- 4) 믿을 수 있는 기관 CA(Certification Authority)가 발행하는 X.509 certificate에는 public key e_B 가 Bob의 public key임을 입증하는 CA의 digital signature가 포함되어 있다. CA의 public key가 (e_a, n_a) 이고, private key가 (d_a, n_a) 이라고 할 때, Bob의 public key e_B 를 인증하는 CA의 digital signature를 계산하시오. (단, hash function은 $H()$ 그리고 encryption 알고리즘은 RSA 알고리즘을 사용한다고 가정한다) (5점)

행정안전부 시험출제과장