

# Adatbiztonság (vihim102)

2. kis zh  
2009 április 20.

## 1. feladat

Milyen szolgáltatásokat nyújt az IPsec/AH (Authentication Header) protokoll? [0.6 pont] Milyen szolgáltatásokat nyújt az IPsec/ESP (Encapsulated Security Payload) protokoll? [0.6 pont] Két tűzfal az egymás közötti HTTP forgalom védelmére az AH protokollt használja *tunnel* módban. Mi lesz a fejlécek sorrendje a két tűzfal között megfigyelhető IP csomagokban? [0.8 pont]

## 2. feladat

Milyen alprotokolljai vannak az SSL-nek, és hogyan helyezkednek ezek el a TCP/IP protokoll stack-ben? [0.4 pont] Milyen feladatokat látnak el az egyes alprotokollok? [1 pont] Milyen információk tartoznak egy SSL session állapotához? [0.6 pont]

## 3. feladat

Vázolja fel két Bluetooth eszköz közötti link kulcs létrehozásának módját! [1 pont] Sorolja fel a Bluetooth biztonsági architektúrájának gyengeségeit! [1 pont]

Érdemjegy: pontszám  $\geq 5 \rightarrow 5$ ;  $4 \leq$  pontszám  $< 5 \rightarrow 4$ ;  $3 \leq$  pontszám  $< 4 \rightarrow 3$ ;  $2 \leq$  pontszám  $< 3 \rightarrow 2$ ; pontszám  $< 2 \rightarrow 1$ ;