**Prezentačná vrstva definuje spôsob, akým aplikácia komunikuje so sieťou. {T}**

**Prezentačná vrstva je určená na priamu komunikáciu s vrstvami sieťovej infraštruktúry. {F}**

**Prezentačná vrstva je špecifikovaná vo všetkých sieťových architektúrach. {F}**

**Prezentačná vrstva nie je zvlášť špecifikovaná v architektúre TCP/IP, ktorú používa internet. {T}**

**Architektúra TCP/IP nemusí implementovať mechanizmy funkcií, ktoré sú špecifikované na prezentačnej vrstve. {F}**

**Konverzia formátov dát na prezentačnej vrstve sa vytvára výlučne špeciálnym jazykom ASN (Abstract Syntax Notation) {F}**

**Aké dve základné metódy kompresie existujú? {**

-Stratová a bezstratová kompresia

**Aké sú výhody metódy TLV? {**

-Správy môžu byť posielané v ľubovoľnom poradí

-Protokol vo formáte TLV sa ľahko rozširuje o nové typy správ

-V jednom datagrame môže byť odoslaný ľubovoľný počet správ v tvare TLV

**Aké sú základné druhy šifrovania? {**

-Asymetrické šifrovanie -Symetrické šifrovanie

**Aké vlastnosti má asymetrické šifrovanie? {**

-Šifruje sa jedným kľúčom, dešifruje sa iným

**Aké sú možné dôvody, že si odosielateľ a príjemca tej istej informácie neporozumejú? {**

-Použitie rôznych kódových stránok

-Spôsob, akým si rôzne procesory alebo programovacie jazyky ukladajú dáta do pamäte

-Rôzny formát dát (hlasu, videa...) -Použitie rôznych metód šifrovania

**Aký je rozdiel medzi kódovými stránkami ISO 8859-2 a Windows 1250? {**

-Obsahujú tú istú abecedu, ale nie sú kompatibilné

**Ako sa komprimácia realizuje v praxi? {**

-Automaticky uložením do súborov, ktoré majú špecifikované komprimované formáty, napríklad JPEG, MPEG, MP3

-Pomocou špeciálnych komprimačných programov, napríklad ZIP, RAR

**Ako sa nazýva veda o šifrovaní a dešifrovaní? {**

-Kryptológia -Kryptografia

**Čo sa označuje pojmom kryptoanalýza? {**

-Veda, ktorá sa zaoberá matematickými postupmi na získanie pôvodného obsahu zašifrovanej informácie

**Čo znamená pojem kryptografia? {**

-Veda, ktorá sa zaoberá prevodom informácie do nečitateľnej podoby

**Čo platí o páre verejného a privátneho kľúča? {**

-Verejný kľúč môže byť zverejnený, privátny musí zostať utajený u vlastníka

-Principiálne sú oba kľúče pri vygenerovaní páru rovnocenné - čo sa zašifruje jedným kľúčom, možno dešifrovať druhým

**Čo je to certifikačná autorita (CA)? {**

-CA vydáva certifikáty pre osoby a servery

**Čo je to token? {**

-Technické zariadenie, v ktorom sa ukladá privátny kľúč majiteľa

**Čo si môžu komunikujúce aplikácie v rámci služieb prezentačnej vrstvy dohodnúť pre prenos dát? {**

-Použitie hlasového kódovania -Kódovanie diakritiky

**Čo to znamená, že je kompresia stratová? {**

-Že v procese kompresie zanedbáva a vypúšťa isté detaily vstupných dát

**Čo obsahuje digitálny certifikát? {**

-Údaje o vlastníkovi certifikátu -Verejný kľúč vlastníka

-Dobu platnosti certifikátu -Digitálny podpis certifikačnej autority

**Čo znamená https vo WWW adrese? {**

-Použitie zabezpečeného (secured) spojenia

**Ktoré z nasledujúcich tvrdení nie sú funkciami prezentačnej vrstvy? {**

-Rozdeľovanie dát na samostatne prenášané segmenty -Riadenie toku dát

**Ktoré z nasledujúcich činností sú funkcie prezentačnej vrstvy? {**

-Identifikácia formátu prenášanej informácie -Kompresia prenášaných dát

**Ktoré z uvedených funkcií sú základné funkcie prezentačnej vrstvy? {**

-Zaistenie rovnakého formátu dát

**Ktoré z uvedených funkcií sú ďalšie funkcie prezentačnej vrstvy určené pre komfort a zlepšenie kvality prenosu? {**

-Kompresia prenášaných dát -Šifrovanie dát -Zabezpečenie prenášaných dát

**Ktoré z vymenovaných princípov sú používané pre zabezpečenie rovnakého formátu? {**

-Zvláštny jazyk dátových štruktúr pre prenos -TLV princíp -MIME štandard

**Kde sa spravidla nachádza funkcia šifrovania v OSI modeli? {**

-Na prezentačnej vrstve

**Ktoré z nasledujúcich tvrdení o MIME je pravdivé? {**

-MIME rozširuje službu e-mailu o nové funkcie (prílohy, diakritika)

-MIME je využívané aj v iných protokoloch pre identifikovanie formátu dát

**Ktoré z týchto pojmov predstavujú spôsoby identifikovania typu obsahu (Content Type)? {**

-MIME (Multipurpose Internet Mail Extensions) -TLV (Type Length Value)

**Ktorý spôsob identifikácie formátu dát je vhodnejší pre binárne protokoly? {**

-TLV

**Kedy sú šifrovacie a dešifrovacie kľúče rovnaké a kedy rozdielne? {**

-Rovnaké sú pri symetrickej šifre, rozdielne sú pri asymetrickej

**Ktorý spôsob identifikácie formátu dát je vhodnejší pre textové protokoly? {**

-MIME

**Ktoré z uvedených kódových stránok sú použiteľné pre slovenskú abecedu? {**

-ISO 8859-2 -Unicode

**Kto generuje verejný kľúč? {**

-Majiteľ príslušného privátneho kľúča

**Kto vydáva digitálne certifikáty? {**

-Certifikačná autorita

**Ktoré kompresné metódy dosahujú vo všeobecnosti vyšší kompresný pomer? {**

-Stratové

**Ktoré z uvedených metód sú používané pri bezstratovej kompresii? {**

-Huffmanovo kódovanie -Lempel-Ziv-Welch (LZW) -Slovníkové metódy

**Ktoré z uvedených formátov používajú stratovú kompresiu? {**

-MP3 -JPEG

**Na akom princípe je založené symetrické šifrovanie? {**

-Pre šifrovanie aj dešifrovanie sa využíva rovnaký kľúč

**Používa sa niekedy dešifrovanie nejakej správy pomocou verejného kľúča? {**

-Áno, ak bola správa zašifrovaná privátnym kľúčom, napr. pri digitálnom podpise

**Správa bola pomocou asymetrickej šifry zašifrovaná verejným kľúčom príjemcu. Dokáže ju odosielateľ dešifrovať? {**

-Nie, nedokáže ju dešifrovať

**V ktorých prenosoch informácie je možné použiť bezstratové metódy? {**

- Video -Audio -Grafika