Ktoré z nasledujúcich tvrdení nie sú funkciami prezentačnej vrstvy? {

~%-50%Dohodnutie formátu prenášanej informácie

~%50%Rozdeľovanie dát na samostatne prenášané segmenty

~%50%Riadenie toku dát

~%-50%Šifrovanie a zabezpečenie dát proti neoprávnenej manipulácii

}

Ktoré z nasledujúcich činností sú funkcie prezentačnej vrstvy? {

~%50%Identifikácia formátu prenášanej informácie

~%-50%Diferencovanie a riadenie dialógov

~%50%Kompresia prenášaných dát

~%-50%Zabezpečenie proti chybám v prenose

}

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

~%25%Použitie rôznych kódových stránok

~%25%Spôsob, akým si rôzne procesory alebo programovacie jazyky ukladajú dáta do pamäte

~%25%Rôzny formát dát (hlasu, videa...)

~%25%Použitie rôznych metód šifrovania

}

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}

Ktoré z uvedených funkcií sú základné funkcie prezentačnej vrstvy? {

=Zaistenie rovnakého formátu dát

~Kompresia prenášaných dát

~Šifrovanie dát

~Zabezpečenie prenášaných dát

}

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

~%-100%Zaistenie rovnakého formátu dát

~%33.333%Kompresia prenášaných dát

~%33.333%Šifrovanie dát

~%33.333%Zabezpečenie prenášaných dát

}

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

~%33.333%Zvláštny jazyk dátových štruktúr pre prenos

~%33.333%TLV princíp

~%33.333%MIME štandard

~%-100%Huffmanov kód

}

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

Ktoré z nasledujúcich tvrdení o MIME je pravdivé? {

~%50%MIME rozširuje službu e-mailu o nové funkcie (prílohy, diakritika)

~%50%MIME je využívané aj v iných protokoloch pre identifikovanie formátu dát

~%-50%MIME je binárny protokol (príkazy MIME nie sú textové)

~%-50%MIME je skratka z Many Inputs Many Outputs

}

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

~%50%MIME (Multipurpose Internet Mail Extensions)

~%50%TLV (Type Length Value)

~%-50%RSA (Rivest Shamir Adleman)

~%-50%DES (Data Encryption Standard)

}

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

~MIME

=TLV

~DES

}

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

=MIME

~TLV

~RSA

}

Aké sú výhody metódy TLV? {

~%33.333%Správy môžu byť posielané v ľubovoľnom poradí

~%33.333%Protokol vo formáte TLV sa ľahko rozširuje o nové typy správ

~%33.333%V jednom datagrame môže byť odoslaný ľubovoľný počet správ v tvare TLV

}

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

~%-50%ASCII

~%-50%ISO 8859-1

~%50%ISO 8859-2

~%50%Unicode

}

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

~Sú totožné a navzájom kompatibilné

=Obsahujú tú istú abecedu, ale nie sú kompatibilné

}

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

~%50%Použitie hlasového kódovania

~%50%Kódovanie diakritiky

~%-50%Použitý linkový alebo sieťový protokol

~%-50%Riadenie toku dát na transportnej vrstve

}

Aké dve základné metódy kompresie existujú? {

=Stratová a bezstratová kompresia

~Symetrická a asymetrická kompresia

~Synchrónna a asynchrónna kompresia

}

Čo to znamená, že je kompresia stratová? {

~Že je nevýhodná v porovnaní s inými kompresnými metódami

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

~Že sa pripravuje jej nahradenie inou, lepšou metódou

}

Ktoré kompresné metódy dosahujú vo všeobecnosti vyšší kompresný pomer? {

=Stratové

~Bezstratové

}

Ktoré z uvedených metód sú používané pri bezstratovej kompresii? {

~%33.333%Huffmanovo kódovanie

~%33.333%Lempel-Ziv-Welch (LZW)

~%33.333%Slovníkové metódy

~%-50%MP3

~%-50%MPEG

}

Ktoré z uvedených formátov používajú stratovú kompresiu? {

~%-50%PNG

~%50%MP3

~%-50%GIF

~%50%JPEG

}

V ktorých prenosoch informácie je možné použiť bezstratové metódy? {

~%33.333% Video

~%33.333% Audio

~%33.333% Grafika

~%-50%Text

~%-50%Štruktúrované dáta

}

Ako sa komprimácia realizuje v praxi? {

~%50%Automaticky uložením do súborov, ktoré majú špecifikované komprimované formáty, napríklad JPEG, MPEG, MP3

~%50%Pomocou špeciálnych komprimačných programov, napríklad ZIP, RAR

~%-50%Vždy je potrebný štandardizovaný komprimačný program, ktorý v prípade potreby zmenšenia objemu dát použijeme.

~%-50%Komprimačné programy používateľ použije len pri rozhodnutiach ukladania do formátov JPEG, MPEG, MP3

}

Kde sa spravidla nachádza funkcia šifrovania v OSI modeli? {

=Na prezentačnej vrstve

~Na relačnej vrstve

~Na transportnej vrstve

~Na sieťovej vrstve

}

Aké sú základné druhy šifrovania? {

~%50%Asymetrické šifrovanie

~%50%Symetrické šifrovanie

~%-50%Analogické šifrovanie

~%-50%Synchrónne šifrovanie

}

Aké vlastnosti má asymetrické šifrovanie? {

=Šifruje sa jedným kľúčom, dešifruje sa iným

~Šifruje aj dešifruje sa rovnakým kľúčom

~Pojem asymetrie sa vzťahuje na výsledok dešifrovania - je iný než pôvodné dáta pred zašifrovaním

}

Ako sa nazýva veda o šifrovaní a dešifrovaní? {

~%50%Kryptológia

~%50%Kryptografia

~%-50%Kódológia

~%-50%Steganografia

}

Čo sa označuje pojmom kryptoanalýza? {

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

~Označenie fázy, v ktorej šifrovací program zisťuje, či použitá šifra je dostatočne bezpečná

~Proces, v ktorom používateľský program zisťuje, či prijaté dáta obsahujú zašifrované časti

}

Čo znamená pojem kryptografia? {

=Veda, ktorá sa zaoberá prevodom informácie do nečitateľnej podoby

~Proces generovania dvojíc kľúčov

~Proces distribúcie kľúčov

~Vydávanie certifikátov

}

Na akom princípe je založené symetrické šifrovanie? {

=Pre šifrovanie aj dešifrovanie sa využíva rovnaký kľúč

~Šifruje sa jedným kľúčom, dešifruje sa iným

~Pojem symetrie sa vzťahuje na výsledok dešifrovania - je rovnaký ako pôvodné dáta pred zašifrovaním

}

Čo platí o páre verejného a privátneho kľúča? {

~%50%Verejný kľúč môže byť zverejnený, privátny musí zostať utajený u vlastníka

~%-50%Oba kľúče je možné zverejniť, privátny kľúč aj tak nebude použiteľný

~%50%Principiálne sú oba kľúče pri vygenerovaní páru rovnocenné - čo sa zašifruje jedným kľúčom, možno dešifrovať druhým

~%-50%Ak je známy verejný kľúč, je k nemu možné ľahko vypočítať príslušný privátny kľúč, aby tvorili pár

}

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

~Rovnaké sú pri asymetrickej šifre, rozdielne sú pri symetrickej

=Rovnaké sú pri symetrickej šifre, rozdielne sú pri asymetrickej

~Rovnaké sú pri šifrovaní, rozdielne sú pri dešifrovaní

~Rozdielne sú pri šifrovaní, rovnaké sú pri dešifrovaní

}

Kto generuje verejný kľúč? {

=Majiteľ príslušného privátneho kľúča

~Ktokoľvek, privátny kľúč si vytvárame podľa potreby k príslušnému verejnému kľúču

}

Kto vydáva digitálne certifikáty? {

=Certifikačná autorita

~Národný bezpečnostný úrad

~Príjemca zašifrovanej správy

}

Používa sa niekedy dešifrovanie nejakej správy pomocou verejného kľúča? {

~Nie, dešifrovať správu možno zásadne len privátnym kľúčom

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

}

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

~Áno, dokáže ju dešifrovať

=Nie, nedokáže ju dešifrovať

}

Čo je to certifikačná autorita (CA)? {

=CA vydáva certifikáty pre osoby a servery

~CA na požiadanie overuje certifikáty, no nevydáva ich

~CA vydáva potvrdenia o kryptografickej bezpečnosti zariadení

}

Čo je to token? {

~Synonymum pre heslo, ktorým sa používateľ prihlasuje k sieti

~Pojem pre verejný kľúč

=Technické zariadenie, v ktorom sa ukladá privátny kľúč majiteľa

}

Čo obsahuje digitálny certifikát? {

~%25%Údaje o vlastníkovi certifikátu

~%25%Verejný kľúč vlastníka

~%25%Dobu platnosti certifikátu

~%25%Digitálny podpis certifikačnej autority

}

Čo znamená https vo WWW adrese? {

=Použitie zabezpečeného (secured) spojenia

~Použitie prepojovaného (switched) spojenia

~Použitie synchrónneho (synchronous) spojenia

}