**Test 8**

1. Ktoré z nasledujúcich tvrdení nie sú funkciami prezentačnej vrstvy?{

* Dohodnutie formátu prenášanej informácie
* **Rozdeľovanie dát na samostatne prenášané segmenty**
* **Riadenie toku dát**
* Šifrovanie a zabezpečenie dát proti neoprávnenej manipulácii

2. Ktoré z nasledujúcich činností sú funkcie prezentačnej vrstvy?{

* **Identifikácia formátu prenášanej informácie**
* Diferencovanie a riadenie dialógov
* **Kompresia prenášaných dát**
* Zabezpečenie proti chybám v prenose

3. 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
* **Použitie rôznych metód šifrovania**

4. Čo definuje prezentačná vrstva?

**Spôsob akým komunikujú so sieťou aplikácie**

5. K čomu je primárne určená prezentačná vrstva?

**Zachovať rovnaký formát dát alebo vykonať potrebnú konverziu**

6. V ktorých sieťových architektúrach je špecifikovaná prezentačná vrstva?

**Osi**

7. Ktoré z uvedených funkcií sú základné funkcie prezentačnej vrstvy? {

* **Zaistenie rovnakého formátu dát**
* Kompresia prenášaných dát
* Šifrovanie dát
* Zabezpečenie prenášaných dát

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

* Zaistenie rovnakého formátu dát
* **Kompresia prenášaných dát**
* **Šifrovanie dát**
* **Zabezpečenie prenášaných dát**

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

* Zvláštny jazyk dátových štruktúr pre prenos
* **TLV princíp**
* **MIME štandard**
* Huffmanov kód

10. Ako sa označuje špeciálny jazyk konverzie formátov dát na prezentačnej vrstve?

**ASN.1**

11. 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**
* MIME je binárny protokol (príkazy MIME nie sú textové)
* MIME je skratka z Many Inputs Many Outputs

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

* **MIME (Multipurpose Internet Mail Extensions)**
* **TLV (Type Length Value)**
* RSA (Rivest Shamir Adleman)
* DES (Data Encryption Standard)

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

* MIME
* **TLV**
* DES

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

* **MIME**
* TLV
* RSA

15. 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 môţe byť odoslaný ľubovoľný počet správ v tvare TLV**

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

* ASCII
* ISO 8859-1
* **ISO 8859-2**
* **Unicode**

17. 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**

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

* **Použitie hlasového kódovania**
* **Kódovanie diakritiky**
* Použitý linkový alebo sieťový protokol
* Riadenie toku dát na transportnej vrstve

19. Aké dve základné metódy kompresie existujú?{

* **Stratová a bezstratová kompresia**
* Symetrická a asymetrická kompresia
* Synchrónna a asynchrónna kompresia

20. 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

21. Ktoré kompresné metódy dosahujú vo všeobecnosti vyšší kompresný pomer?{

* **Stratové**
* Bezstratové

22. Ktoré z uvedených metód sú používané pri bezstratovej kompresii? {

* **Huffmanovo kódovanie**
* **Lempel-Ziv-Welch (LZW)**
* **Slovníkové metódy**
* MP3
* MPEG

23. Ktoré z uvedených formátov používajú stratovú kompresiu?{

* PNG
* **MP3**
* GIF
* **JPEG**

24. V ktorých prenosoch informácie je možné použiť bezstratové metódy? {

* Video
* Audio
* **Grafika**
* **Text**
* **Štruktúrované dáta**

25. 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**
* Vždy je potrebný štandardizovaný komprimačný program, ktorý v prípade potreby zmenšenia objemu dát pouţijeme.
* Komprimačné programy používateľ použije len pri rozhodnutiach ukladania do formátov JPEG, MPEG, MP3

26. Kde sa spravidla nachádza funkcia šifrovania v OSI modeli?{

* **Na prezentačnej vrstve**
* Na relačnej vrstve
* Na transportnej vrstve
* Na sieťovej vrstve

27. Aké sú základné druhy šifrovania?{

* **Asymetrické šifrovanie**
* **Symetrické šifrovanie**
* Analogické šifrovanie
* Synchrónne šifrovanie

28. 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 neţ pôvodné dáta pred zašifrovaním

29. Ako sa nazýva veda o šifrovaní a dešifrovaní?{

* Kryptológia
* **Kryptografia**
* Kódológia
* Steganografia

30. 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

31. Čo znamená pojem kryptografia?{

* **Veda, ktorá sa zaoberá prevodom informácie do nečitateľnej podoby**
* Proces generovania dvojíc kľúčov
* Proces distribúcie kľúčov
* Vydávanie certifikátov

32. 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

33. Čo platí o páre verejného a privátneho kľúča?{

* **Verejný kľúč môže byť zverejnený, privátny musí zostať utajený u vlastníka**
* Oba kľúče je moţné zverejniť, privátny kľúč aj tak nebude pouţiteľný
* Principiálne sú oba kľúče pri vygenerovaní páru rovnocenné - čo sa zašifruje jedným kľúčom, moţno dešifrovať druhým
* **Ak je známy verejný kľúč, je k nemu moţné ľahko vypočítať príslušný privátny kľúč, aby tvorili pár**

34. 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

35. Kto generuje verejný kľúč?{

* **Majiteľ príslušného privátneho kľúča**
* Ktokoľvek, privátny kľúč si vytvárame podľa potreby k príslušnému verejnému kľúču

36. Kto vydáva digitálne certifikáty?{

* **Certifikačná autorita**
* Národný bezpečnostný úrad
* Príjemca zašifrovanej správy

37. Používa sa niekedy dešifrovanie nejakej správy pomocou verejného kľúča?{

* Nie, dešifrovať správu moţno zásadne len privátnym kľúčom
* **Áno, ak bola správa zašifrovaná privátnym kľúčom, napr. pri digitálnom podpise**

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

* Áno, dokáţe ju dešifrovať
* **Nie, nedokáţe ju dešifrovať**

39. Čo je to certifikačná autorita (CA)?{

* **CA vydáva certifikáty pre osoby a servery**
* CA na poţiadanie overuje certifikáty, no nevydáva ich
* CA vydáva potvrdenia o kryptografickej bezpečnosti zariadení

40. Čo je to token?{

* Synonymum pre heslo, ktorým sa pouţívateľ prihlasuje k sieti
* Pojem pre verejný kľúč
* **Technické zariadenie, v ktorom sa ukladá privátny kľúč majiteľa**

41. Čo obsahuje digitálny certifikát?{

* **Údaje o vlastníkovi certifikátu**
* **Verejný kľúč vlastníka**
* **Dobu platnosti certifikátu**
* **Digitálny podpis certifikačnej autority**

42. Čo znamená https vo WWW adrese?{

* **Použitie zabezpečeného (secured) spojenia**
* Použitie prepojovaného (switched) spojenia
* Použitie synchrónneho (synchronous) spojenia