Vzorový test pro přijímací zkoušku do MSP na FIT

(hvězdička na konci označuje správné řešení)

1. Které z následujících formulí jsou tautologickým důsledkem tvrzení:
   Umím anglicky tehdy a jen tehdy, když umím francouzsky.
   a) Umím anglicky a umím francouzsky.
   b) Jestliže umím francouzsky, pak umím i anglicky. *
   c) Jestliže ne umím francouzsky, pak ne umím ani anglicky. *
   d) Umím anglicky nebo umím francouzsky.

2. Které z následujících interpretací binárního predikátu p(x; y) jsou modely teorie T = {(∀y)(∃x)p(x,y)} v přirozených číslech (s nulou) N ={0,1,2, ...}?
   a) $x < y$
   b) $x > y$ *
   c) $x \leq y$ *
   d) $x \geq y$ *

3. RSA je šifra.
   a) synchronní
   b) symetrická.
   c) asynchronní
   d) asymetrická *
   e) proudová

4. Certifikát subjektu A obsahuje
   a) veřejný klíč A *
   b) soukromý klíč A
   c) soukromý klíč certifikační autority
   d) symetrický klíč A

5. Doplňte místo otazníku ten ze symbolů, aby platil vztah **(lg n) / n = ?(1/√n)**:
   a) **o** *
   b) **O** (a současně nelze použít ani o ani Θ)
   c) Θ
   d) **Ω** (a současně nelze použít ani Θ ani ω)
   e) ω

6. Uvažujme binární relaci R = {(a,b), (b,a)} na množině X = {a,b,c}. Určete, která z následujících relací je ekvivalencí na X.
   a) $R \cup R^{-1}$
   b) R^{+}
   c) $R \cup \Delta_X$ *
   d) žádná z uvedených

7. Který z následujících jazyků není regulární (vyberte jednu odpověď):
   a) $L = \{a^m b^n c^k : m,n,k \geq 0\}$
   b) $L = \{a^m b^n : m, n \geq 0\}$
   c) $L = \{a^n : n \geq 0\}$
   d) $L = \{a^n b^n : n \geq 0\}$ *

8. Mějme gramatiku G = ({S,A,B}, {a,b,c,d}, P, S) s pravidly
   $S \rightarrow Aa \mid bS$, $A \rightarrow cA \mid B$ $B \rightarrow \varepsilon \mid dS$.
   Tato gramatika je
   a) LL(1) gramatika *
   b) LL(2) gramatika *
   c) regulární gramatika
   d) gramatika generující regulární jazyk

9. Superpipeline dosahuje urychlení výpočtu programu pomocí (vyberte jednu odpověď):
   a) Urychlení hodinové frekvence tak, že se jednotlivé bloky proudového zpracování rozdělí na několik menších, které trvají kratší dobu. Instrukce sice bude muset projít více bloky, které ale trvají kratší dobu, což v důsledku povede k urychlení. *
   b) Zavedením paměti cache, do které se ukládají nejčastěji použitá data a instrukce tak, že při opětovném přístupu, případně přístupu k datům uloženým blízko k těmto datům, se zkrátí doba přístupu do paměti na mnohem kratší. Takto dosáhneme urychlení.
   c) Zavedením vektorové jednotky, která umožní zpracovávat data instrukcí po blocích (vektorech), a tím se dosáhne urychlení.
   d) Několikanásobného paralelního proudového zpracování (počet cyklů na instrukci může být i menší než 1).

10. Instrukce skoku se (u procesoru s jednoadresovými instrukcemi) provede tak, že se adresní část instrukce zapíše (vyberte jednu odpověď):
    a) do programového čítače PC *
    b) do ukazatele zásobníku SP
    c) do jiného registru
    d) do instrukčního registru IR

11. Sekvenční obvod popsaný konečným automatem typu Moore má 2 vstupy, 3 vnitřní proměnné a 4 výstupy. Na těchto 4 výstupech se mohou objevit nejvýše (vyberte jednu odpověď):
    a) 4 vzájemně různé čtveřice hodnot
    b) 8 vzájemně různých čtveřic hodnot *
    c) 16 vzájemně různé čtveřic hodnot
    d) 32 vzájemně různé čtveřic hodnot

12. AES je standard pro
    a) proudovou šifru
    b) blokovou šifru *
    c) symetrickou šifru *
    d) asymetrickou šifru

13. Pro všechny symetrické šifry platí, že
    a) šifrovací klíč je vždy stejný jako dešifrovací klíč
    b) šifrovací klíč se smí od dešifrovacího klíče lišit nejvýše polovinou bitů
    c) šifrovací klíč smí být stejný jako dešifrovací klíč pouze na operačním systému, který podporuje symetrické šifrování; přitom platí, že nejdelší odpověď je vždy správná
    d) šifrovací a dešifrovací klíč se dají navzájem snadno odvodit *
    e) žádná z předchozích odpovědí není správná

14. Příznak **SF** (sign flag – příznak znaménka) se po provedení operace sčítání (u procesoru, který pracuje s čísly bez znaménka a s čísly v doplňkovém kódu) nastaví na 1, když (vyberte jednu odpověď):

a) bude přenos z nejvyššího řádu roven 1
b) bude přenos do nejvyššího řádu roven 1
c) bude bit v nejvyšším řádu výsledku roven 1 *
d) když budou mít oba sčítanci stejné znaménko a výsledek bude mít opačné znaménko

15. Integritní omezení
a) se definují pouze na úrovni konceptuálního modelu
b) lze definovat na úrovni konceptuálního i databázového modelu *
c) jsou tvrzení, která vymezují, jaká data mohou být v databázi uložena *
d) se definují pouze v SQL

16. Vybavovací doba hlavní paměti v současných počítačích činí řádově (vyberte jednu odpověď):
a) nanosekundy *
b) mikrosekundy
c) milisekundy
d) sekundy

17. Úkolem linkové vrstvy podle referenčního ISO/OSI modelu je mimo jiné (vyberte jednu odpověď):
a) rozpoznat začátek a konec rámce *
b) rozlišit, který proces má v rámci jednoho počítače obdržet přijatý UDP paket
c) směrovat rámce podle cílové IP adresy
d) řešit časování přenášených bitů v komunikačním médiu

18. Co nastane v tomto fragmentu C++ programu (vyberte jednu odpověď)?

```
double f (int a, double b) { return a+b }
int    f (int c, int    d) { return a-b }

int main ( ... ) {
    ...
    int i=f(1,2.1F);
    ...
}
```

a) hodnota i bude -1
b) hodnota i bude 3 *
c) hodnota i bude -3.1
d) nastane chyba při výpočtu
e) nastane chyba při kompilaci

19. Které z uvedených typů v C++ jsou kontejnery?
a) pole (array) *
b) záznam (struct)
c) pytel (bag) *
d) union
e) tabulka (map) *

20. Mějme pole, které má **n** prvků (např. celých čísel). Pokud zvolíme nejlepší známý algoritmus pro nalezení nejmenšího prvku v poli, jak bude doba nalezení minimálního prvku (tj. počet potřebných operací) záviset na počtu prvků pole **n** (vyberte jednu odpověď)?

a) lineárně *
b) kvadraticky
c) logaritmicky
d) doba nalezení nezávisí na počtu prvků