Kryptológia – test (7.1.2004) **A**

1. Ak by sme v Needhamovom-Schroederovom protokole nahradili výskyty príležitostných slov časovými pečiatkami, tak by bol protokol bezpečný.
   ☐ áno ☐ nie

2. Ak by sme v jednoduchej substitučnej šifre nepoužívali kľúče (permutácie) s pevnými bodmi, tak by bol jednoduchší
   A. útok s možnosťou voľby otvoreného textu
   B. útok úplným preberaním
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

3. Uvažujme dvojité šifrovanie $E_{k_2}(E_{k_1}(m))$. Máme k dispozícii niekoľko dvojíc otvorených a šifrových textov šifrovaných rovnakými kľúčmi. Potom vieme implementovať útok úplným preberaním tak, že má asymptoticky rovnakú
   A. časovú zložitosť ako pri jednoduchom šifrovaní
   B. pamäťovú zložitosť ako pri jednoduchom šifrovaní
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

4. Uvažujme RSA systém, kde $n = pq$ je verejný modulus.
   A. verejný exponent e je rôzny od p aj q
   B. každý šifrový text je nesúdeliteľný s n
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

5. Pre ľubovoľný jazyk z **P**
   A. existuje perfektný bezznalostný interaktívny dokazovací systém.
   B. existuje interaktívny dokazovací systém, v ktorom sa overovateľ pre ľubovoľný vstup nikdy nemýli.
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

6. Ak by sme vedeli triediť porovnávaním v lineárnom čase, tak zložitosť „narodeninovho“ útoku sa
   ☐ zmenší ☐ nezmení ☐ zväčší

7. Útok na RSA využívajúci schopnosť získať pre ľubovoľný šifrový text hodnotu paritného bitu otvoreného textu, viedol k
   A. faktorizácii n
   B. získaniu súkromného exponentu d
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

8. Nech **XIP** je trieda jazykov, ktoré majú taký interaktívny dôkazovací systém, v ktorom sa overovateľ nikdy nemýli.
   A. **XIP** je uzavretá na prienik
   B. **XIP** je uzavretá na zreťazenie
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

9. Uvažujme schému pre slepé podpisy založenú na RSA.
   A. Ak použijeme namiesto správy jej hašovanú hodnotu, schéma nebude fungovať.
   B. Ak podpisujúci vie efektívne faktorizovať, vie zistiť, k akej správe chce druhý účastník získať podpis.
   ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

10. Pri analýze protokolu v BAN logike
    A. nešifrované časti správ neovplyvňujú analýzu
    B. ak účastník nemá žiadne úvodné viery (predpoklady), tak po skončení protokolu tiež nebude mať žiadne viery
    ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

11. V grupe $(\mathbb{Z}_7^*, \cdot)$ zvoľme generátor $g = 3$. Nech verejný kľúč v ElGamalovom systéme je $y = 6$. Potom dešifrovaná podoba šifrového textu $(2, 2)$ je

    . . . . . .

12. V oblivious transfer protokole je potrebné zabezpečiť vlastnosť:
    ☐ jednosmernosť
    ☐ odolnosť voči kolíziám
    ☐ jednoznačnosť
    ☐ žiadne

13. Pohligov-Hellmanov algoritmus pre výpočet diskrétneho logaritmu je efektívny, ak
    A. rád grupy je malý
    B. rád grupy má iba malé prvočíslené faktory
    ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

14. Určte hodnotu Legenderovho symbolu $(\frac{3}{7})$.
    ☐ -1 ☐ 0 ☐ 1

15. Uvažujme nebijektívnu hašovaciu funkciu $H : \{0,1\}^{256} \to \{0,1\}^{256}$.
    A. Ak pre všetky x platí $H(x) \in \{0^{256}, 1^{256}\}$, tak H je jednosmerná.
    B. Ak pre všetky $x \leq y$ platí $H(x) \leq H(y)$, tak H nie silne odolná voči kolíziam.
    ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

16. Ak budeme pre inštanciu RSA systému šifrovať takto: $E(m) = m^{(e^2)} \bmod n$, tak je možné dešifrovať takto: $D(c) = c^{(d^2)} \bmod n$.
    ☐ áno ☐ nie

17. Upravme Shamirovu (t, n) schému na zdieľanie tajomstva tak, že účastník P_i vždy dostane ako podiel hodnotu polynómu v bode i.
    A. schéma ostane perfektná
    B. schéma ostane ideálna
    ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

18. V Rabinovom asymetrickom šifrovacom systéme má šifrovacia transformácia tvar $E(m) = m^2 \bmod n$, kde n je súčin dvoch rôznych prvočísel.
    A. jednému šifrovému textu zodpovedá viacero otvorených textov
    B. jednému otvorenému textu zodpovedá viacero šifrových textov
    ☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

19. Zmena 1 bitu otvoreného textu môže potenciálne ovplyvniť všetky bloky šifrového textu v móde
    ☐ ECB ☐ OFB ☐ CFB ☐ žiadne

20. Na Diffieho-Hellmanov protokol možno útočiť útokom
☐ meet in the middle
☐ opakovaním
☐ man in the middle
☐ „narodeninovým“

21. Vypíšte všetky kvadratické nerezíduá modulo 12:

. . . . . .

22. V bit commitment schéme založenej na probléme diskrétneho logaritmu musí byť výpočtovo obmedzený (aby bola schéma bezpečná)
☐ tvorca commitmentu
☐ príjemca commitmentu
☐ obaja
☐ nikto

23. Uvažujme Goldwasserov-Micaliho pravdepodobnostný systém. Ten každý bit šifruje ako náhodné QR_n (bit 0) alebo QNR_n (bit 1). Ak útočník
A. vie faktorizovať n, tak vie rozbiť tento systém
B. má nejaké QR_n, tak vie invertovať jednotkové bity v šifrovom texte
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

24. Označme E šifrovací algoritmus. Potom vlastnosť $\forall k_1 \forall k_2 \exists k_3 \forall m$: $E_{k_1}(E_{k_2}(m)) = E_{k_3}(m)$
A. platí pre premutačnú šifru
B. platí pre Vernamovu šifru
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

25. Uvažujme ElGamalovu schému pre digitálne podpisy, pričom nepoužijeme hašovaciu funkciu.
A. Každej správe prislúcha viac ako jeden platný digitálny podpis.
B. Schopnosť falšovať náhodnú správu vedie k prezradeniu súkromného kľúča.
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne