Kryptológia – test (3.2.2004) **A**

1. Wide-mouthed frog protokol
A. nie je bezpečný, lebo šifrované správy sú symetrické
B. by bol bezpečný po nahradení časových pečiatok príležitostnými slovami
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

2. Určte minimálnu dĺžku správy nad abecedou $\{0, 1\}$, keď množina kľúčov permutačnej šifry je väčšia ako množina kľúčov Vernamovej šifry

....

3. Uvažujme vzdialenosť jednoznačnosti otvoreného textu (označme t) pre jednoduchú substitučnú šifru nad abecedou s r znakmi.
A. Ak rastie entropia jazyka, t klesá.
B. Pre ľubovoľný jazyk platí $t \leq r$.
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

4. Uvažujme RSA systém, kde $n = pq$ je verejný modulus dĺžky 2004 bitov.
A. ak $E(m) = m$, tak aj $E(m^{2004}) = m^{2004}$
B. ak je otvorený text QR_n, tak aj šifrový text je QR_n
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

5. Každý jazyk z **NP** má IDS, v ktorom dokazovateľ pošle práve jednu správu.
☐ áno ☐ nie

6. Každá bijektívna funkcia je
A. jednosmerná
B. slabo odolná voči kolíziám
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

7. Uvažujme RSA systém, kde $n = pq$ je verejný modulus.
A. Ak $p - 1$ alebo $q - 1$ majú len dva prvočíslené faktory, vieme n efektívne faktorizovať.
B. Znalosť faktorizácie je ekvivalentná znalosti súkromného exponentu d.
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

8. Uvažujme bezznalostný interaktívny dokazovací systém (ZK IDS) pre izomorfizmus grafov. Tento ZK IDS je
A. perfektný
B. jednosmerný
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

9. Falšovanie náhodnej správy (random message forgery) je útok na schémy digitálnych podpisov, pri ktorom útočník
A. získa súkromný kľúč používateľa
B. z podpisu k správe m dokáže vytvoriť podpis k správe m^2
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

10. Pri analýze protokolu v BAN logike
A. viery účastníkov iba pribúdajú
B. sa príležitostné slová vo fáze idealizácie vynechávajú
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

11. Uvažujme inštanciu ElGamalovho asymetrického šifrovacieho systému pre prvočíslo p a generátor g grupy $(\mathbb{Z}_p^*, \cdot)$.
A. existuje otvorený text, ktorému zodpovedá práve jeden šifrový text
B. existuje dvojica $\langle r, s\rangle$, kde $r, s \in \mathbb{Z}_p$, ktorá nemôže vzniknúť šifrovaním žiadneho otvoreného textu
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

12. Pravdepodobnostný charakter mala simulácia
A. 1-2 oblivious transfer pomocou 50% OT
B. 50% oblivious transfer pomocou 1-2 OT
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

13. Nech $p > 2$ je prvočíslo a g je generátor grupy $(\mathbb{Z}_p^*, \cdot)$. Pre ľubovoľné $b \in \mathbb{Z}_p^*$ vieme určiť ...... diskrétneho logaritmu b pri základe g.
☐ prvý bit
☐ posledný bit
☐ žiadny bit

14. Asmuthova-Bloomova schéma na zdieľanie tajomstva je
A. ideálna
B. perfektná
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

15. Nech H je hašovacia funkcia. Ak H^2 má vlastnosť $\mathcal{X}$, tak aj H má vlastnosť $\mathcal{X}$.
A. $\mathcal{X}$: silne odolná voči kolíziám
B. $\mathcal{X}$: jednosmerná
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

16. Dešifrovanie v RSA systéme (modul $n = pq$) s využitím Čínskej zvyškovej vety
A. sa používa na urýchlenie dešifrovania.
B. využíva znalosť prvočísel p a q.
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

17. Trieda monotónnych prístupových štruktúr (pre schémy na zdieľanie tajomstva) je uzavretá na
A. prienik
B. doplnok
☐ 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. každému šifrovému textu zodpovedajú štyri rôzne otvorené texty
B. náhodný padding (vypchávka) zabraňuje útoku s možnosťou voľby šifrového textu
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

19. Zmena 1 bitu šifrového textu ovplyvní po dešifrovaní všetky následné bloky otvoreného textu v móde
☐ CBC ☐ OFB ☐ CFB ☐ žiadne

20. Problém získania kľúča pre spojenie pasívnym útočníkom v Diffieho-Hellmanovom protokole je ekvivalentný problému rozbitia asymetrického systému
☐ RSA
☐ BBS
☐ Rabinovho
☐ žiadne

21. Nech $p > 2$ je prvočíslo.
A. existuje $b \in \mathbb{Z}_p^*$ také, že $(\frac{b}{p}) = (\frac{b+1}{p})$
B. $p - 2$ je QR_p
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

22. Ak by výpočet bit commitment nezahŕňal voľbu náhodného reťazca, tak by bola schéma napadnuteľná
A. tvorcom commitmentu
B. príjemcom commitmentu
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

23. Uvažujme BBS generátor s modulom $n = pq$.
A. perióda generátora je vždy menšia ako $n/2$
B. ak počiatočnú hodnotu generátora zvolíme $n - 1$, generovaná postupnosť bude mať periódu 1
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

24. Uvažujme Vernamovu šifru.
A. dĺžka kľúča je rovnaká ako dĺžka správy
B. kľúče sú volené rovnako pravdepodobne
☐ A aj B ☐ iba A ☐ iba B ☐ žiadne

25. Počet modulárnych umocnení pri podpisovaní v ElGamalovej schéme je
☐ 0 ☐ 1 ☐ 2 ☐ 3