Doplnkové cvičenie (2025)

Testové otázky

1. Vzájomný index koincidencie reťazcov ‘abab’ a ‘cbcb’ je . . . . . .
2. Index koincidencie textu ‘abab’ je . . . . . .
3. Vzdialenosť jednoznačnosti otvoreného textu sa zmenšuje so zmenšujúcou sa entropiou kľúča.

   ☐ áno ☐ nie
4. Two-time pad problém nás potenciálne trápi pri

   ☐ CBC ☐ OFB ☐ ECB
5. Meet-in-the-middle útok na trojité šifrovanie s troma nezávislými kľúčmi má časovú zložitosť $\sim 2^X$, kde X je

   ☐ n ☐ $2n$ ☐ $3n$ ☐ $4n$
6. Slide útok vyžaduje, aby útočník mohol zvoliť otvorené texty na šifrovanie (CPA).

   ☐ áno ☐ nie
7. Ktorý mód obvykle používa výplň (padding)?

   ☐ CBC ☐ OFB ☐ CFB ☐ CTR
8. GCM mód autentizovaného šifrovania využíva na šifrovanie mód

   ☐ CBC ☐ OFB ☐ CFB ☐ CTR
9. V RSA schéme je súkromný exponent d nesúdeliteľný s $\varphi(n)$.

   ☐ áno ☐ nie
10. V RSA schéme asymetrického šifrovania použitie Čínskej vety o zvyškoch urýchľuje šifrovanie.

    ☐ áno ☐ nie
11. Ak vieme efektívne riešiť DLOG problém v danej grupe, tak vieme efektívne riešiť aj výpočtový Diffieho-Hellmanov problém v tejto grupe.
    ☐ áno ☐ nie
12. Šifrový text v ElGamalovej schéme je dvojica (r, s). Z týchto hodnôt závisia na otvorenom texte:
    ☐ obe hodnoty ☐ iba r ☐ iba s ☐ žiadna
13. Narodeninový útok na hašovaciu funkciu hľadá
    ☐ vzor ☐ druhý vzor ☐ kolíziu
14. HMAC spracuje každý blok vstupnej správy dvakrát.
    ☐ áno ☐ nie
15. Podpisy v ECDSA sú oproti ElGamalovej schéme pri rovnakej úrovni bezpečnosti
    ☐ kratšie ☐ dlhšie ☐ rovnako dlhé
16. PBKDF2 používa okrem hesla ako vstup aj soľ.
    ☐ áno ☐ nie
17. V Regevovej schéme využívajúcej LWE (Learning with Errors) problém nad $\mathbb{Z}_q$ je otvorený text volený z množiny
    ☐ $\{0, 1\}$ ☐ $\mathbb{Z}_q$ ☐ $\left\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\right\}$
18. Merkleho-Damgårdova konštrukcia hašovacej funkcie zabezpečí, že výsledná hašovacia funkcia je odolná voči kolíziám, ak je odolná voči kolíziám použitá kompresná funkcia.
    ☐ áno ☐ nie
19. Podpisová schéma RSA PKCS#1 v1.5 je
    ☐ deterministická ☐ znáhodnená

20. V Merkleho podpisovej schéme (MSS) očakávame, že výpočtovo náročnejšie je
☐ overenie podpisu ☐ podpísanie správy

21. Na PBKDF2 funkcii použitej na ukladanie hesiel nám z hľadiska ochrany pred slovníkovým útokom môže prekážať
☐ nízka pamäťová zložitosť
☐ nemožnosť paralelizovať výpočet
☐ obmedzená dĺžka výstupu

22. Falšovanie náhodnej správy nás nemusí trápiť pri Schnorrovej podpisovej schéme.
☐ áno ☐ nie

23. Uvažujme Hellmanovu tabuľku pre hľadanie hesiel z ich odtlačku. Transformácie odtlačku na heslo sú
☐ rôzne pre každý stĺpec ☐ rôzne pre každý riadok ☐ rovnaké pre každý riadok aj stĺpec

24. Nech H je hašovacia funkcia odolná voči kolíziám. Potom aj $G(x) = H(x) \oplus H(\overline{x})$ je odolná voči kolíziám.
☐ áno ☐ nie

25. Merkleho podpisová schéma využívajúca strom hĺbky k (koreň má hĺbku 0) umožňuje podpísať
☐ 1 správu ☐ k správ ☐ 2^k správ ☐ $2^{k+1} - 1$ správ

26. Použitie soli pri ukladaní hesiel má za cieľ:
☐ spomaliť výpočet odtlačku pri slovníkovom útoku
☐ znemožniť útok hrubou silou
☐ spomaliť útočníka pri on-line hádaní hesiel
☐ znemožniť predvýpočet odtlačkov hesiel vopred.

27. Zložitosť dešifrovania v Regevovej schéme (založenej na LWE probléme, s dĺžkou súkromného kľúča/vektora n) je
☐ $O(\log n)$ ☐ $O(n)$ ☐ $O(n \log n)$ ☐ $O(n^2)$

28. Nech h je dĺžka výstupu hašovacej funkcie a k je dĺžka kľúča. Potom dĺžka výstupu HMAC skonštruovaného z tejto hašovacej funkcie je
☐ h ☐ $h + k$ ☐ $2h$ ☐ $2h + k$ ☐ žiadne z predchádzajúcich

Príklady

1. Navrhnite techniku ciphertext stealing pre ECB mód. Predpokladáme, že správa je dlhšia ako jeden blok. Očakávame, že (1) počet volaní E_k pri šifrovaní OT sa nezmení (2) technika nepoužije žiadnu XOR operáciu. Popíšte šifrovanie aj dešifrovanie v tomto prípade.
2. Uvažujme AES v CFB móde, v ktorom použijeme výplňovú schému (napriek tomu, že to nie je potrebné), napr. ako v PKCS #7. Popíšte, ako by prebiehal oracle padding útok a čo by ním útočník dosiahol.
3. V "učebnicovej" verzii RSA šifrovacej schémy nám prekážal determinizmus šifrovania. Rozhodnite a zdôvodnite vhodnosť nasledujúcich úprav, využívajúcich náhodne vyberaný znáhodňujúci faktor $r \xleftarrow{\$} Z_n^*$. Šifrový text k otvorenému textu $m \in Z_n$ je
   (a) $(r^e \bmod n, r + m \bmod n)$;
   (b) $(r, (rm)^e \bmod n)$.
4. Určte interval, v akom sa môže pohybovať vzdialenosť jednoznačnosti pre Vigenereovu sifru s dĺžkou kľúča 4, ak abeceda jazyka otvoreného textu má 32 znakov.
5. (Curveball 2020) Verejný kľúč používateľa v ECDSA schéme je $Q = dG$, kde $d \in \mathbb{Z}_n^*$ je súkromný kľúč (n je prvočíselný rád podgrupy bodov eliptickej krivky generovanej generátorom G). Ukážte ako môže ktokoľvek vytvoriť falošný podpis používateľa A k ľubovoľnej správe m, ak príjemca akceptuje ako parameter schémy ľubovoľné G' (ostatné parametre schémy zostanú nezmenené).
6. Nech E je bloková šifra (povedzme AES-128). Predpokladajme, že dĺžka správy je vždy násobkom dĺžky bloku (označme správu m rozdelenú na bloky takto: $m = m_1, m_2, \ldots, m_n$). Zdôvodnite, prečo nasledujúce konštrukcie nie sú vhodné ako MAC:
   a) $H_k(m) = (c_0, c_n)$, kde c_n je posledný blok získaný šifrovaním m pomocou E_k v CFB móde a c_0 je náhodne zvolený IV,
   b) $G_k(m) = E_{m_n}(\ldots E_{m_2}(E_k(m_1))\ldots)$, kde predpokladáme, že v E je dĺžka bloku zhodná s dĺžkou kľúča,
   c) $F_k(m) = E_k(m_1) \oplus E_k(E_k(m_2)) \oplus \ldots \oplus E_k^n(m_n)$.
7. Nech g je generátor grupy $(\mathbb{Z}_p^*, \cdot)$, kde p je veľké prvočíslo. Nech správa m je rozdelená na bloky $m = m_1, m_2, \ldots, m_n$, kde každé $m_i \in \mathbb{Z}_p$. Rozhodnite a zdôvodnite, či sú nasledujúce konštrukcie hašovacích funkcií odolné voči kolíziám:
   a) $H(m) = h_n$, kde $h_i = g^{h_{i-1}+m_i}$ a $h_0 = 0$;
   b) $H(m) = h_n$, kde $h_i = g^{m_i} \cdot h_{i-1}$ a $h_0 = 2020$.