Cvičenie 2 (30.11.2022)

Testové otázky

1. Narodeninový útok na hašovaciu funkciu hľadá
   ☐ vzor ☐ druhý vzor ☐ kolíziu

2. HMAC spracuje každý blok vstupnej správy dvakrát.
   ☐ áno ☐ nie

3. Podpisy v DSA sú oproti ElGamalovej schéme pri rovnakej úrovni bezpečnosti
   ☐ kratšie ☐ dlhšie ☐ rovnako dlhé

4. PBKDF2 používa okrem hesla ako vstup aj soľ.
   ☐ áno ☐ nie

5. V Regevovej schéme využívajúcej LWE (Learning with Errors) problém nad $\mathbb{Z}_q$ je otvorený text volený z množiny
   ☐ $\{0,1\}$ ☐ $\mathbb{Z}_q$ ☐ $\left\{-\frac{q-1}{2},\ldots,\frac{q-1}{2}\right\}$

6. Merkleho-Damgårdova konštrukcia hašovacej funkcie zabezpečí, že výsledná hašovacia funkcia je odolná voči kolíziám, ak je odolná voči kolíziám použitá kompresná funkcia.
   ☐ áno ☐ nie

7. Podpisová schéma RSA PKCS#1 v1.5 je
   ☐ deterministická ☐ znáhodnená

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

9. 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

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

11. Uvažujme McElieceovu schému asymetrického šifrovania. Schéma nebude bezpečná, ak použitý samoopravný kód opravuje najviac 1 chybu.
    ☐ áno ☐ nie

12. 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

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

14. 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

15. 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.

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

17. 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. (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).

2. 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) $F_k(m) = E_k(m_1) \oplus E_k(E_k(m_2)) \oplus \ldots \oplus E_k^n(m_n)$.

3. Rozhodnite a zdôvodnite, či sú bezpečné nasledujúce varianty Schnorrovej podpisovej schémy (používame označenie zhodné s prednáškou; samozrejme, potrebné je upraviť aj overovaciu rovnicu):

   a) V podpise je inak počítaná hodnota $s = k + r + x \bmod q$ (r sa nezmení).
   b) V podpise je inak počítaná hodnota $s = k - rx \bmod q$ (r sa nezmení).

4. V Goldreichovej podpisovej schéme použijeme strom, v ktorom má každý nelistový vrchol 4 potomkov. Podpisovať budeme odtlačky správ dĺžky 256 bitov.

   a) Popíšte ako bude fungovať podpisovanie a overovanie podpisov v novej schéme.
   b) Porovnajte dĺžky verejného kľúča, súkromného kľúča a podpisu správy v pôvodnej a novej schéme. Predpokladajte, že v použitých jednorazových podpisových schémach je v dĺžka verejného kľúča, s dĺžka súkromného kľúča a p dĺžka podpisu.
   c) Porovnajte časovú zložitosť podpisovania v oboch schémach. Nech g je zložitosť generovania schémy a nech f je zložitosť podpisu.

5. 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 $h_0 = 2020$.

6. Nech má útočník v McElieceovom systéme šifrový text $c = mG' + e$, pričom $\mathrm{wt}(e) \leq t$. Predpokladajme, že útočník dokáže podhodiť ľubovoľný šifrový text c' a následne rozlíšiť podľa reakcie adresáta, či je v c' najviac t chýb a text sa dešifruje na m (situácia A), alebo je v ňom viac ako t chýb, prípadne dešifrovaný otvorený text nie je m (situácia B). Popíšte a zdôvodnite postup, ako pomocou orákula rozhodujúceho situácie A a B odstrániť z c chybový vektor e, teda určiť $x = mG'$. Určte počet potrebných dotazov na orákulum v najhoršom prípade.
   Pomôcka: Rozdeľte postup na dve časti. V prvej sa z c vyrobí c^*, ktoré má presne $t + 1$ chýb vzhľadom na x.