Cvičenie 1 (27.10.2021)

Testové otázky

1. Vzájomný index koincidencie reťazcov ‘abab’ a ‘cbcb’ je ... ...

2. Vzdialenosť jednoznačnosti otvoreného 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. Najkratší LFSR (posuvný register s lineárnou spätnou väzbou) generujúci postupnosť ‘011111’ má dĺžku ……

10. Korelačný útok na prúdovú šifru je primárne útok typu
    ☐ COA ☐ KPA ☐ CPA

11. V RSA schéme je súkromný exponent d nesúdeliteľný s $\varphi(n)$.
    ☐ áno ☐ nie

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

13. Vypíšte všetky prvky množiny QR_{13}: _____

14. Ak vieme efektívne riešiť DLOG problém v danej grupe, tak vieme efektívne riešiť aj výpočtový Diffieho-Hellmanov problém v tejto grupe.
    ☐ áno ☐ nie

15. Šifrový text v ElGamalovej schéme je dvojica (r, s). Z týchto hodnôt závisia na otvorenom texte:
    ☐ obe hodnoty ☐ iba r ☐ iba s ☐ žiadna

Príklady

1. Popíšte slide útok na variant šifry Speck-2n, v ktorej je v každom kole použitý rovnaký kľúč (zhodný s kľúčom šifry). Dĺžka kľúča je teda n bitov a nech má šifra n kôl. Akú zložitosť bude mať tento útok (dátovú aj časovú) – porovnajte s útokom hrubou silou? Vedeli by Ste útok vylepšiť v CPA scenári – ako?

2. 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.

3. 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.

4. Uvažujme aditívnu prúdovú šifru postavenú nad LFSR (so známou spätnou väzbou) dostatočnej dĺžky n. Popíšte, zdôvodnite očakávanú zložitosť čo najlepšieho KPA útoku rekonštruujúceho vnútorný stav.
   (a) Bežiaci kľúč je konštruovaný ako každý druhý výstupný bit LFSR.
   (b) Bežiaci kľúč obsahuje bit 1 vtedy, keď je počet 1 bitov LFSR párny (v opačnom prípade má bit hodnotu 0).

5. 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) $(r, (rm)^e \bmod n)$.

6. Určte interval, v akom sa môže pohybovať vzdialenosť jednoznačnosti pre Vigenereovu sifru s dĺžkou kľúča 4, ak abeceda jazyka otvoreného textu má 32 znakov.