3 marca 2021

Zadania z kryptografii, lista nr 2

1. Przypomnij znane Ci algorytmy mnożenia długich liczb całkowitych. Jaka jest ich złożoność, jeśli rozmiarem problemu jest długość mnożonych liczb l.

2. *Redukcja Montgomery'ego* służy do wyliczania $a^x \bmod n$, gdy n jest długą liczbą naturalną. Niech $l = \lceil \log_2 n \rceil, r = 2^l \perp n$ i $r'r - n'n = 1$. Za pomocą redukcji Montgomery'ego znając A i B wyliczamy $t = ABr' \bmod n$. Używamy następującego algorytmu:

   - $T \leftarrow A \cdot B$,
   - $m \leftarrow Tn' \bmod r$,
   - $t' \leftarrow (T + mn)/r$,
   - zwróć $t = t'$ lub $t = t' - n$, w zależności od tego, które z nich jest w $\mathbb{Z}_n$.

   Uzasadnij poprawność redukcji Montgomery'ego. Jaka jest jej złożoność obliczeniowa? W jaki sposób może być ona użyta do szybkiego wyliczenia $a^x \bmod n$?

3. Niech $\bar{x}$ będzie logicznym dopełnieniem ciągu x złożonego z zer i jedynek. Niech E oznacza szyfrowanie DESem. Pokaż, że jeśli $y = E_K(x)$, to $\bar{y} = E_{\bar{K}}(\bar{x})$. Jak używając tej tożsamości można zredukować dwukrotnie liczbę szyfrowań przy kryptoanalizie DESa poprzez przeszukanie przestrzeni kluczy dla danej pary tekst jawny – szyfrogram?

4. Określ złożoność ataku 'meet in the middle' na 3-krotny i 4-krotny DES.

5. Przy przesyłaniu szyfrogramu w DES nastąpiło przekłamanie jednego bitu. Ile bitów tekstu jawnego zostało utraconych jeśli DESa użyto w trybie ECB, CBC, CFB, OFB, k-CFB, k-OFB, CTR.

6. W których trybach działania DES można wykryć, że po raz drugi przesłany został szyfrogram tej samej wiadomości, a w których nie?

7. Pokaż, że istnieje dokładnie $(n-1)!$ permutacji długości n, w których 1 jest w cyklu długości k. Jaka jest średnia długość cyklu zawierającego 1 w losowej permutacji? Jaka jest średnia liczba iteracji trybu OFB dla której następuje powtórzenie bloku r_i ciągu losowego generowanego przez ten tryb? Jak można oszacować średnią długość cyklu w trybie k-OFB dla k mniejszego od długości bloku?

8. Niech $\mathbb{Q}$ będzie ciałem liczb wymiernych. Niech $\mathbb{Q}[\sqrt{2}]$ będzie zbiorem liczb w postaci $a + b\sqrt{2}$ gdzie a i b są liczbami wymiernymi.

   (a) pokaż że dla różnych par a, b liczby $a + b\sqrt{2}$ są różne

   (b) pokaż, że $\mathbb{Q}[\sqrt{2}]$ jest ciałem z dodawaniem i mnożeniem.