Kryptografia

Lista nr 6, 27 V

1. Przyjmijmy, że dla dowolnych grafów X, Y jesteś w stanie efektywnie znajdować izomorfizm $f : X \to Y$ między nimi (o ile te grafy są izomorficzne). Zaproponuj dowód z wiedzą zerową znajomości f.
2. Zaproponuj dowód z wiedzą zerową dla znajomości cyklu Hamiltona.
3. Zaproponuj dowód z wiedzą zerową dla znajomości faktoryzacji modułów RSA (tj. takich $N = pq$, gdzie p, q pierwsze).
4. Niech $G(x) = a_1x + b_1 \bmod p_1$, $H(x) = a_2x + b_2 \bmod p_2$. Pokaż, że RSA-OAEP z powyżej zdefiniowanymi funkcjami G i H nie jest CCA-Secure.
5. Załóż, że masz dostęp do wyroczni, która na wejściu c będącym kryptogramem (książkowego) RSA wiadomości m, odpowiada jaki jest najmniej znaczący bit m. Pokaż jak wykorzystać wyrocznię do całkowitego zdeszyfrowania c.
6. Zaproponuj modyfikację algorytmu szyfrowania ElGamala polegającą na zmianę grupy Z_p na Z_n, gdzie $n = pq$ dla pewnych liczb pierwszych p, q. Czy takie rozwiązanie jest bezpieczne?
7. Powiemy, że x jest pierwiastkiem kwadratowym y modulo n jeżeli $x^2 \equiv y \bmod n$ (wtedy y nazywamy resztą kwadratową modulo n).

   Pokaż, że dla liczby pierwszej p liczba pierwiastków kwadratowych $y \in Z_p^*$ jest równa 2 albo 0.
8. Ile jest pierwiastków kwadratowych dla $n = pq$, gdzie p, q są liczbami pierwszymi?
9. Pokaż, że dla liczby pierwszej $p > 2$ zbiór reszt kwadratowych tworzy podgrupę w Z_p^*. Jaki jest rozmiar tej podgrupy?
10. Zaproponuj efektywny algorytm obliczania pierwiastków kwadratowych w Z_n.
11. Niech $n = pq$ dla $p \equiv q \equiv 3 \bmod 4$, gdzie p, q są liczbami pierwszymi.

    Pokaż, że jeżeli dla dowolnego $c \in QR(n)$ umiemy wyliczać takie $r \neq s$, że $s^2 \equiv (n - s)^2 \equiv r \equiv (n - r)^2 \equiv c \bmod n$ to potrafimy znaleźć p, q.
12. Z przecieku z prokuratury dowiedziano się, że jeden z członków trzyosobowego zarządu pewnej partii został oskarżony o branie łapówek. Wiadomo jedynie, że zawiadomienie o możliwości popełnienia przestępstwa zostało zgłoszone, wiadomo przez kogo, ale nie wiadomo kto jest podejrzanym.

    Zarząd spotyka się na spotkaniu i musi ustalić strategię:

    - pozwanie oskarżającego (jeżeli nikt z zarządu łapówki nie wziął),
    - dyskredytowanie/zastraszanie oskarżającego i zamiatanie sprawy pod dywan (jeżeli któryś z członków zarządu łapówkę przyjął).

    Z uwagi na walki między frakcjami w partii, nikt kto wziął łapówkę nie przyzna się do tego pozostałym członkom zarządu.

    Twoim zadaniem jest zaproponowanie protokołu, który pozwoli na przyjęcie właściwej strategii. Wynikiem protokołu ($F(x_1, x_2, x_3)$) ma być stwierdzenie czy któryś spośród nich wziął łapówkę ($F = 1$) czy nie ($F = 0$). Protokół ma zapewniać "anonimowość": uczestnik i nie może poznać x_j dla $j \neq i$. Możesz założyć uczciwość uczestników protokołu (dobro partii dobrem najwyższym). Jak wygląda złożoność obliczeniowa i komunikacyjna protokołu?