Lista zadań. Nr 9. 22 maja 2005

Kryptografia

IIUWr.

1. Opracuj protokół wymiany informacji pomiędzy Alicją a Bobem, który przekona Boba, że dla danych a, b i liczby pierwszej p, Alicja zna wartość $x = log_a b \bmod p$ i jednocześnie nie wyjawi żadnej informacji na temat x (lub przynajmniej jak najmniej informacji o x).

2. Opracuj dowód interakcyjny dla problemu nieizomoficzności grafów. Czy Twój dowód jest z wiedzą zerową?

3. Dokończ rozpoczęty na wykładzie dowód następującego faktu: jeśli Ewa zna wartość γ, przy której prawdopodobieństwo skutecznego podszycia się za Alicję w schemacie uwierzytelniania Okamoto jest co najmniej $1/2^{t-1}$, gdzie t jest parametrem bezpieczeństwa, to współpracując z Alicją, Ewa może z prawdopodobieństwem $1 - 1/q$ obliczyć $\log_{\alpha_1} \alpha_2$.

4. Protokół zobowiązania bitowego wykonywany przez Alicję i Boba polega na tym, że

   - Alicja wybiera losowo bit b, koduje go i jako m przekazuje Bobowi,
   - Bob nie jest w stanie odczytać z m, czy Alicja wybrała 0 czy 1,
   - w odpowiedniej chwili Alicja odkrywa b poprzez odpowiednie obliczenia na m.

   Ważne jest, by Alicja nie mogła oszukać Boba i zmienić wartość b już po przekazaniu m Bobowi. Jak zrealizować zobowiązanie bitowe, mając:

   (a) algorytm szyfrowania symetrycznego;

   (b) jednostronne funkcje hashujące.

5. Wykorzystaj protokół zobowiązania bitowego, do skonstruowania protokołu "losowania monety przez telefon".

6. Rozważmy pewien hipotetyczny schemat identyfikacji. Alicja ma tajny klucz $n = pq$, gdzie p i q są liczbami pierwszymi oraz $p \equiv q \equiv 3(\bmod 4)$. Alicja posiada wydany przez TA certyfikat na wartość n. Gdy Alicja chce się przedstawić (powiedzmy Bobowi), ten przekazuje jej losową resztę kwadratową x modulo n. Wtedy Alicja oblicza pierwiastek kwadratowy y liczby x i przesyła wynik Bobowi. Bob sprawdza, czy $y^2 \equiv x \bmod n$. Wyjaśnij, dlaczego ten schemat nie jest bezpieczny.

7. Przedstaw schemat uwierzytelniania Guillou-Quisquatera.

8. Wykonaj wszystkie zadania rachunkowe znajdujące się na końcu rozdziału 9 książki Stinsona.