Lista zadań. Nr 5. 1 kwietnia 2005

Kryptografia

IIUWr.

1. (1pkt) Pokaż, że ostatni bit tekstu jawnego zaszyfrowanego RSA jest "tak samo bezpieczny" jak cały tekst. Dokładniej: pokaż, że Ewa dysponująca procedurą znajdującą ostatni bit tekstu jawnego na podstawie kryptogramu oraz klucza publicznego, potrafiłaby w prosty sposób otrzymać cały tekst jawny. Co możesz powiedzieć o bezpieczeństwie innych bitów?

2. (2pkt) (Oszukiwanie w pokerze przez telefon) Rozważ ponownie protokół gry w pokera przez telefon opartego na RSA. W pierwszym etapie gracze umawiają się co do wartości liczbowych reprezentujących poszczególne karty. Wybór losowych liczb wydaje się być sensowny. Czy jednak w takim przypadku informacja o kartach przeciwnika jest dobrze ukryta?

   Wskazówka: Zastanów się, jakie cechy liczb nie są "zakrywane" przez funkcję szyfrującą w RSA.

3. (1pkt) (Niebezpieczeństwo używania małego wykładnika szyfrującego) Atrakcyjnym kluczem szyfrującym w RSA jest $e = 3$, ponieważ wówczas szyfrowanie jest bardzo szybkie. Załóżmy, że Alicja chce rozesłać tę samą wiadomość m do trzech przyjaciół Boba, Charliego i Davida używających $e_B = e_C = e_D = 3$ dla różnych n_B, n_C, n_D. Pokaż, jak Ewa może odszyfrować m po przechwyceniu jej szyfrogramów.

4. (2pkt) (Inne niebezpieczeństwo związane z małym wykładnikiem szyfrującym) Załóżmy, że Ewa dysponuje dwoma kryptogramami c_1 i c_2 otrzymanymi przez zaszyfrowanie tym samym kluczem RSA wiadomości m i $m + 1$. Pokaż, w jaki sposób Ewa potrafi odczytać m.

5. (2,5pkt) Czy potrafisz rozszerzyć metodę Ewy z poprzedniego zadania na sytuację, w której teksty jawne, których kryptogramami dysponuje Ewa, powiązane są ogólniejszą (np. liniową) zależnością.

6. (2pkt) Wiadomość m jest punktem stałym dla krryptosystemu RSA, gdy $m^e \equiv m \bmod n$. Pokaż, że liczba punktów stałych kryptosystemu RSA wynosi $gcd(e - 1, p - 1) \cdot gcd(e - 1, q - 1)$.