2 Kolokwium: Kryptografia 2005
zadania przykładowe
WPPT PWr, M.Kutyłowski

Odpowiedz zwięźle na arkuszu z pytaniami. Odpowiedź powinna dotyczyć jądra zagadnienia. **Każda odpowiedź musi być UZASADNIONA. Odpowiedź tak/nie traktowana jest na 0 punktów.**

W każdym zadaniu można zdobyć 3 punkty. Można korzystać z własnych notatek, wydruków, ... W przypadku braku pseudonimu wynik będzie podany z numerem indeksu.

---

1. Jak przeprowadzić atak różnicowy na DES, jeśli możemy wprowadzić błędy do układu obliczającego kryptogramy DESa do inputu 15 rundy?

2. Próbujemy zastosować atak saturacyjny do DES-a. Lewą połówkę inputu nasycamy, prawa jest ustalona. Czy po trzeciej rundzie prawa połówka jest nasycona?

3. Załóżmy, że potrafimy określić za pomocą poboru energii ile jedynek zostało wyliczonych w trakcie ostatniej rundy DESa. Jak zdobyć klucz używany do szyfrowania przsy pomocy tych informacji?

4. Zaproponuj mechanizmy, które możnaby wbudować w funkcję hashującą aby uodpornić na atak różnicowy. Można się nie przejmować za bardzo pogorszeniem czasu obliczeń.

5. Możemy wykonywać hashowanie dwóch bloków 512-bitowych jednocześnie przy pomocy dwóch układów elektronicznych. Zaproponuj schemat, który wykorzystałby to do szybszego hashowania dużych plików.

6. Pokaż, że w A5/1 istnieją stany wewnętrzne rejestrów, dla których nie ma poprzedników. Oszacuj ich liczbę.

7. W A5/1 zastąpiono regułę większości przez OR. Czy taki układ jest łatwiejszy do złamania? Dlaczego?

8. Zaproponuj kanał kleptograficzny, którym możnaby przesyłać informacje do osoby wybranej spośród k ustalonych osób.

9. Zaproponuj podpisy pierścieniowe, świadczące o tym, że dwie różne osoby z pierścienia składały podpis.

10. Dla podpisów niezaprzeczalnych, jakie jest prawdopodobieństwo odrzucenia dobrego podpisu Alicji w procedurze odrzucania, jeśli Alicja oszukuje?

11. Jak zaprojektować system CA, aby zdobycie przez adwersarza prywatnych kluczy dwóch CA nie powodowało niemożności sprawdzenia ważności podpisu cyfrowego.