14.01.03

KRYPTOGRAFIA I BEZP. KOMP.,
WPPT, INF. INŻ. 2002

Lista zadań nr 4

1. Generator LFSR jest przewidywalny w tym sensie, że jeśli poznamy wystarczajaco dużo bitów na wyjściu, to możemy przewidzieć jego wyjścia od tego miejsca.

- Jak przeprowadzić ten atak, gdy liczba rejestrów LFSR nie jest znana?
- Czy wykonywanie działań nie na bitach, lecz np. bajtach polepszy bezpieczeństwo działania LFSR?
- Czy znając odpowiednio długi blok k wyjść można wyliczyć wszystkie bity na wyjściu, które wystąpiły przed tym blokiem?

2 • Wybierz odpowiedni schemat uzgadniania kluczy pomiędzy Alicja a Bobem tak aby był odporny na atak typu *replay*, tzn. taki, w którym osoba podszywająca się pod Alicję powtarza podsłuchane kiedyś komunikaty wysłane przez Alicję (bez łamania tych kryptogramów).

- Podaj przykłady protokołów nieodpornych na tego typu ataki.
- Wybierz odpowiedni protokół uzgadniania klucza gwarantujący, że klucze będą wybierane losowo przez obie strony.

3. Jedna z metod obrony przez atakiem *man-in-the-middle* polega na tym, że Alicja przesyła połowę kryptogramu. Potem Bob przesyła połowę kryptogramu odpowiedzi (nie wiedząc jeszcze co Alicja powiedziała), po czym Alicja przesyła drugą połowę kryptogramu, Bob przesyła drugą połowę kryptogramu odpowiedzi. Itd.
Metoda ta zwana *przeplataniem*, opiera się na tym, że *man-in-the-middle* nie jest w stanie przekodowywać połówek kryptogramów.
Wyspecyfikuj dokładnie metodę bezpiecznego logowania się przy pomocy takiego protokołu. Przeprowadź analizę bezpieczeństwa.

4. Czy protokół MTI jest odporny na atak *man-in-the-middle*? Uzasadnij.

5. Po co w ssh stosuje się jednocześnie dwa klucze publiczne serwera? W jaki sposób ssh broni się przed atakiem typu *reply*?

6. Przeanalizuj dlaczego w Kerberosie osoba podsłuchująca komunikaty w sieci nie może ich wykorzystać do ataku. Rozważ możliwie wiele potencjalnych zagrożeń.

7. Zaprojektuj protokół komunikacyjny między Alicją a Bobem, w którym przy minimalnym dodatkowym koszcie można zapewnić, że niepostrzeżenie nikt nie będzie w stanie dorzucić komunikatów ani usunąć. Alicja i Bob nie szyfrują swoich wiadomości. Wskazówka: spojrzeć na specyfikację SSL.

/-/ Mirosław Kutyłowski