2.11.03

KRYPTOGRAFIA I BEZPIECZEŃSTWO

WPPT 2003, INFORMATYKA INŻYNIERSKA

Zadania przygotowawcze na kolokwium nr 1

1. Kubuś i Tygrysek ścigają się, kto lepiej rozwiąże niniejszą listę. Ten kto zrobi mniej zadań funduje lody. O godzinie 12 przesyłają sobie swoje zadania a potem dyskutują nad rozwiązaniami.
   Tygrysek podejrzewa Kubisia, że ten po otrzymaniu emaila od Tygryska skopiuje do swego listu brakujące rozwiązania i dopiero wtedy prześle swoje rozwiązania.
   Poradź Kubusiowi i Tygryskowi jak rozwiązać wątpliwości tego typu.
2. Bolek przechwycił zadania na kolokwium zaszyfrowane metodą one-time pad. Pragnie je sprzedać. Jaką cenę możnaby mu zaoferować? Jakie informacje można odczytać z kryptogramu?
3. Efekt lawinowy opisano jako: *zmiana pojedynczego bitu klucza powoduje zmianę każdego bitu kryptogramu.* To prawda czy fałsz? Dlaczego?
4. Efekt lawinowy nie zachodzi dla one-time pad. Dlaczego więc stosujemy tą metodę?
5. Koziołek Matołek słyszał, że nie należy wielu danych szyfrować tym samym kluczem. Wpadł więc na pomysł: każdy plik na swoim dysku szyfruje DES-em przy pomocy losowo wybranego klucza. Jednak aby móc odszyfrować, do każdego pliku dołącza kryptogram z użytym kluczem. W tym wypadku stosuje one-time pad. Czy metoda ta jest dobra Twoim zdaniem? Czy zrobiłbyś tak samo?
6. **Do pomyślenia:** Na rynek wchodzi firma *CheapPhone* oferująca telefony GSM, w których algorytm A5 uproszczono - zamiast skomplikowanej reguły przesuwania rejestrów LFSR zawsze przesuwane są rejestry.
   Pokaż, że ze stosunkowo niewielkiego początkowego fragmentu generowanego ciągu pseudolosowego można odtworzyć cały generowany ciąg.
7. Alicja i Bob mają software realizujący tryb szyfrowania ECB. Słyszeli o niebezpieczeństwach ECB, jednak nie chce im się pisać software'u realizującego CBC. Słyszeli, że można się uchronić przed atakiem omawianym na wykładzie poprzez odpowiednie przekształcenie szyfrowanego tekstu. Jak powinni to zrobić?
8. **Do pomyślenia**: Funkcja hashująca może być zrealizowana za pomocą dobrego algorytmu blokowego w trybie CBC. Zastanów się jak to zrobić.
9. Czy schemat Feistela wymaga aby zastosowana funkcja była wzajemnie jednoznaczna?
10. Co się stanie, gdy w trybie CBC podczas szyfrowania jednego bloku wystąpi błąd? Ile bloków kryptogramu ulegnie zmianie? Które bloki tekstu jawnego da się poprawnie odczytać?
11. Tryb ECB uzupełniono o tzw. „whitening“: tekst jawny T przed zaszyfrownaniem XOR-uje się z tekstem „Pana Tadeusza“ (zapisanym w ASCII). Czy stanowi to dobrą obronę przed przedstawionym na wykładzie atakiem na ECB?
12. W pewnej aplikacji klucz dla 3-DESa tworzony jest jako $SHA-1$(czas sytemowy). przeanalizuj złożoność ataku *brute force* (tj. przeglądanie wszystkich możliwych kluczy) na tak tworzone kryptogramy.
13. Jak deszyfrować w RC5? Wyprowadź odpowiednie wzory.
14. Dlaczego algorytmu IDEA nie da się zaimplementować zamieniając słowa 16-bitowe słowami 32-bitowymi?
15. Implementując schemat szyfrowania ElGamala parametr k wybierany jest tak by się nie powtórzył: najpierw i potem $i+1$, $i+2$ itd. Czy jest to bezpieczny sposób? Uzasadnij wskazując atak bądź jakiś dowód bezpieczeństwa.

/-/ Mirosław Kutyłowski