26.03.02

Kryptografia i bezpieczeństwo

WPPT 2002, informatyka inżynierska

Zadania przygotowawcze na kolokwium

1. Transfer plików zazwyczaj realizuje się przy pomocy szyfrowania hybrydowego. Porównaj ze zwykłym szyfrowaniem symetrycznym i asymetrycznym i znajdź zalety trybu hybrydowego.
2. Dlaczego schemat Feistela umożliwia deszyfrowanie bez odwracania funkcji?
3. Efekt lawinowy opisano jako: *zmiana pojedynczego bitu klucza powoduje zmianę każdego bitu kryptogramu.* To prawda czy fałsz? Dlaczego?
4. Co się stanie, gdy w trybie CBC w jednym bloku wystąpi błąd?
5. Oceny z kolokwium szyfrowane i przechowywane są w trybie ECB. Opisz atak umożliwiający otrzymanie bdb bez konieczności uczenia się (oprócz materiału dotyczącego ECB, oczywiście).
6. Oszacować jakiej wielkości klucze jesteśmy w stanie łamać metodą brute force, jeśli w 1 sek. potrafimy zaszyfrować 1 milion bloków.
7. Porównaj podatność na atak brute-force algorytmów DES i 3-DES.
8. Bolek przechwycił zadania na kolokwium zaszyfrowane metodą one-time pad. Pragnie je sprzedać. Jaką cenę możnaby mu zaoferować?
9. Pokazać, że ciąg generowany przez LFSR jest okresowy. Czy jeśli LFSR ma n jednobitowych rejestrów, to okres może być równy 2^n?
10. Ciag pseudolosowy możnaby generować za pomocą dobrego algorytmu blokowego w trybie CBC. Jak?
11. MAC (powiedzmy 4 bajtowy) możnaby generować za pomocą dobrego algorytmu blokowego w trybie CBC. Jak?
12. Jak dobrać wielkość salt, aby atak słownikowy na hasła nie miał praktycznie znaczenia?
13. Zrealizować zobowiązanie bitowe przy pomocy (a) funkcji hashującej, (b) szyfrowania asymetrycznego.
14. Zadanie z gwiazdką: Jak grać w karty w wojnę przez telefon?
15. Oszacować złożoność ataku urodzinowego przy funkcji hashującej o wartościach złożonych z 40 bitów.
16. Czy jeśli pomnożymy dwa podpisy RSA, to dostaniemy podpis RSA? Dlaczego użycie funkcji hashującej w podpisach jest mocno zalecane?
17. Co się stanie, gdy w wiadomości podpisywanej podpisem RSA dopiszemy jedno zero na końcu wiadomości?
18. Jakie są szanse na udowodnienie zastosowania przez Alicję i Boba kanału podprogowego w podpisach ElGamala? Jak się bronić przed jego odkryciem?

/-/ Mirosław Kutyłowski