20.11.02

Kryptografia i bezpieczeństwo

WPPT 2002, informatyka inżynierska

Zadania przygotowawcze na kolokwium nr 1

1. Bolek przechwycił zadania na kolokwium zaszyfrowane metodą one-time pad. Pragnie je sprzedać. Jaką cenę możnaby mu zaoferować? Jakie informacje można odczytać z kryptogramu?
2. Transfer plików zazwyczaj realizuje się przy pomocy szyfrowania hybrydowego. Jednym z celów jest nieszyfrowanie tym samym kluczem dużej porcji danych. Jak ten cel mogą osiągnąć Alicja i Bob do prowadzonej między sobą komunikacji, jeśli mogą korzystać z szyfrowania symetrycznego.
3. MAC (powiedzmy 4 bajtowy) możnaby generować za pomocą dobrego algorytmu blokowego w trybie CBC. Jak?
4. Ciąg pseudolosowy możnaby generować za pomocą dobrego algorytmu blokowego w trybie CBC. Jak?
5. Dlaczego schemat Feistela umożliwia deszyfrowanie bez odwracania funkcji? Wytłumacz na czym polega sztuczka.
6. Efekt lawinowy opisano jako: *zmiana pojedynczego bitu klucza powoduje zmianę każdego bitu kryptogramu.* To prawda czy fałsz? Dlaczego?
7. Co się stanie, gdy w trybie CBC w jednym bloku wystąpi błąd? Ile bloków kryptogramu ulegnie zmianie? Które bloki tekstu jawnego da się poprawnie odczytać?
8. Tryb ECB uzupełniono o „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?
9. W pewnej aplikacji klucz dla 3-DESa tworzony jest jako H(czas sytemowy). zanalizuj złożoność ataku *brute force* na tak tworzone klucze.
10. Kryptoanaliza różnicowa opiera się na efekcie, że jeśli przed XOR-owaniem z podkluczem między dwoma tekstami jest różnica R to po XOR-owaniu rożnica pozostaje taka sama. Aby uniknąć tego ataku zastąpiono XOR z podkluczem 48 bitowym przez dodawanie modulo 2^{48}. Oceń skuteczność takiego podejścia.
11. Napisz automat stanowy dla „ładowalnej karty telefonicznej". Tj. takiej, która zmniejszłaby saldo pod wpływem impulsów z odpowiedniego automatu telefonicznego i mogłaby być ładowana z odpowiedniego automatu do ładowania. Wybierz odpowiednie metody autoryzacji.
12. Implementując schemat 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.
13. Pokazać, że dla $x, y < n$ x, y względnie pierwszych z n, $x \cdot y \bmod n$ jest też względnie pierwsze z n.
14. Dla $n = pq^2$, p, q - pierwsze, policzyć ile jest liczb naturalnych $x < n$ względnie pierwszych z n.
15. Kod MAC dołączony do tekstu nie realizuje wszystkich funkcji podpisu własnoręcznego. Wymień te funkcje, które spełnia i te których nie spełnia. Uzasadnij krótko dla każdej funkcji.
16. Dla schematu podpisów z wykorzystaniem RSA z n 1024-bitowym oraz z hashowaniem 160 bitowym: jakie jest prawdopodobieństwo, że losowo wybrany ciąg jest podpisem Alicji? (pod jakimkolwiek dokumentem)

/-/ Mirosław Kutyłowski