Kodowanie i bezpieczeństwo informacji

Lista nr 4 na 12 III - 23 III 2012

Zadanie 1 Posiadasz dwie funkcje haszujące f i g. Wiesz, że jedna z nich jest *collision-resistant*, a druga nie, ale nie wiesz która jest która. Twoim zadaniem jest stworzenie nowej funkcji haszującej, która jest *collision-resistant*. Uzasadnij, która z poniższych funkcji będzie odporna na kolizje lub wskaż kontrprzykład ($||$ oznacza konkatenację).

- $h(x) = f(x)||g(x)$,
- $h(x) = f(g(x))$,
- $h(x) = f(g(x))||g(f(x))$.

Zadanie 2 Funkcja haszująca powinna być odporna na kolizje i pseudolosowa. Czy któraś z tych własności jest mocniejsza niż druga? Dla każdej z implikacji wykaż prawdziwość bądź podaj kontrprzykład.

1. jeżeli funkcja jest *collision-resistant*, to jest też pseudolosowa,
2. funkcja pseudolosowa jest odporna na kolizje.

Zadanie 3 Oszacuj prawdopodobieństwo, że są dwa nieidentyczne pliki mające tę samą wartość MD5. Powtórz to dla SHA-1.

Zadanie 4 Udowodnij, że tryby szyfrowania CBC, OFB i Counter Mode nie są odporne na atak chosen ciphertext bez względu na to jaką funkcję F wykorzystamy.

Zadanie 5 Co się stanie gdy w trybie CBC podczas szyfrowania jednego bloku nastąpi błąd? Ile bloków kryptogramu ulegnie zmianie? Które bloki tekstu jawnego da się odczytać? Wyjaśnij co się stanie gdy wykorzystaliśmy tryb CBC do szyfrowania dysku.

Zadanie 6 Tryb ECB uzupełniono o „whitening": tekst jawny M przed zaszyfrowaniem XOR-uje się z tekstem „Pana Tadeusza" (zapisanym w ASCII). Czy tak zmodyfikowany tryb szyfrowania jest odporny na *chosen plaintext attack*?

Zadanie 7 Oceny z kolokwium są szyfrowane i przechowywane w trybie ECB. Opisz atak umożliwiający otrzymanie oceny bardzo dobrej bez konieczności uczenia się do kolokwium.

Zadanie 8 Oszacować jakiej wielkości klucze jesteśmy w stanie łamać metodą *brute force*, jeśli w ciągu jednej sekundy potrafimy zaszyfrować 1 miliard bloków. Ile potrzebujemy czasu aby złamać DES, 3-DES a ile aby złamać AES-128/192/256?

Zadanie 9 W pewnej aplikacji klucz dla 3-DES tworzony jest jako $md5(\text{czas systemowy})$. Przeanalizuj złożoność ataku *brute force* (tj. przeglądanie wszystkich możliwych kluczy) dla tak stworzonych kryptogramów. Jak zmieni się złożoność ataku gdy zamiast 3-DES będzie AES-128/192/256 bitowy a jako funkcję haszującą zostanie wykorzystane SHA-0/SHA-1/SHA-256?