Kolokwium 2: Kryptografia 2005

WPPT, M.Kutyłowski, **grupa A**

Nazwisko i imię: .....

numer indeksu: ..... wydział: .....

pseudonim: .....

Odpowiedz zwięźle na arkuszu z pytaniami. Odpowiedź powinna dotyczyć jądra zagadnienia. **Każda odpowiedź musi być UZASADNIONA. Odpowiedź tak/nie traktowana jest na 0 punktów.**

W każdym zadaniu można zdobyć 3 punkty. Można korzystać z własnych notatek, wydruków, ... W przypadku braku pseudonimu wynik będzie podany z numerem indeksu.

1. W celu ochrony przed atakiem różnicowym przeprowadzanym poprzez generownie błędów zwiększono liczbę rund w DESie z 16 do 32. W jakim stopniu zmieni się złożoność ataku?

2. Zaproponować system oparty o X.509, pozwalający sprawdzić, że klucz publiczny Alicji nie został unieważniony, nawet jeśli dowolne dwa CA zostały zniszczone przez adwersarza.

STRONA NA BRUDNOPIS

3. W A5/1 zastąpiono regułę większości przez XOR. Czy taki układ jest łatwiejszy do złamania? Dlaczego?

4. Napisz pełną specyfikację tworzenia podpisów pierścieniowych dla pierścienia wielkości 3.

5. Załóżmy, że serwer A ustala klucz sesyjny, szyfruje go kluczem publicznym osoby, z którą nawiązuje połączenie, i przesyła jej uzyskany kryptogram publicznym kanałem. Jak zbudować kanał kleptograficzny tak aby dodatkowo Bob poznawał te klucze?

6. Budując funkcję hashującą mamy do wyboru dwie opcje:

   (a) każdy bit hashowanego bloku wykorzystywany jest w operacjach jedynie raz,

   (b) każdy bit wykorzystywany jest wielokrotnie.

   Która opcja daje większą odporność na kryptoanalizę różnicową?

Kolokwium 2: Kryptografia 2005

WPPT, M.Kutyłowski, **grupa B**

Nazwisko i imię: .....

numer indeksu: ..... wydział: .....

pseudonim: .....

Odpowiedz zwięźle na arkuszu z pytaniami. Odpowiedź powinna dotyczyć jądra zagadnienia. **Każda odpowiedź musi być UZASADNIONA. Odpowiedź tak/nie traktowana jest na 0 punktów.**

W każdym zadaniu można zdobyć 3 punkty. Można korzystać z własnych notatek, wydruków, ... W przypadku braku pseudonimu wynik będzie podany z numerem indeksu.

1. Napisz specyfikację weryfikacji podpisu w przypadku potwierdzania klucza publicznego w systemie SPKI.

2. Załóżmy, że algorytm szyfrowania symetrycznego zaimplementowano w ten sposób, że operacje wykonywane na ciągach bitowych, które mogą być wykonywane równolegle, są wykonywane jedocześnie. Załóżmy, że pobór energii dla wykonania operacji XOR zależy głównie od wyniku tej operacji. Zbuduj na tej podstawie atak na DES lub Rijndael.

STRONA NA BRUDNOPIS

3. Wskaż wszystkie stany rejestrów A5/1, które pozwalają na wygenerowanie ciągu 0100.

4. Zbuduj kanał kleptograficzny dla algorytmu Diffie-Hellmana tak, aby Alicja myślała, że jest jedyną osobą korzystającą z kanału, natomiast w istocie dostęp do informacji miał również Bob.

5. Dla zwiększenia odporności algorytmu DES na ataki kryptoanalityczne zamiast obliczać $\mathrm{DES}_K(T)$ obliczamy $\mathrm{DES}_K(T \text{ XOR } K_1)$, gdzie K, K_1 są kluczami szyfrowania. W jaki sposób wpływa to na odporność algorytmu wobec kryptoanalizy różnicowej.

6. W schemacie podpisów niezaprzeczalnych przedstawionym na wykładzie Bob podsłuchuje przebieg weryfikacji podpisu pod m między Alicją a Celiną, a następnie próbuje wykorzystać uzyskane informacje dla podszycia się pod Alicję i zweryfikowanie podpisu pod $m^2 \mod p$ wobec Roberta. Dlaczego nie jest to możliwe?