Kolokwium: Kryptografia - zestaw testowy
WPPT & Wydział Elektroniki & UWr M.Kutyłowski

Nazwisko i imię: .....
numer indeksu: .....
pseudonim: .....

Odpowiedz zwięźle na arkuszu z pytaniami. Odpowiedź powinna dotyczyć jądra zagadnienia. W każdym zadaniu można zdobyć 3 punkty.

Niniejsze zadania są trudniejsze niż na kolokwium zaliczeniowym.

1. Czy możliwe jest szyfrowanie tekstów k-bitowych kluczami $k-1$-bitowymi tak, aby każdy kryptogram mógł odpowiadać każdemu tekstowi jawnemu (tak jak w przypadku one-time-pad)?

2. Czy istnieje n, będące iloczynem różnych liczb pierwszych takie, że istnieje 9 pierwiastków z jedności modulo n?

3. W metodzie rho Pollarda faktoryzacji n kolejna wygenerowana wartość x_j testowana jest w parze z wartością x_k, gdzie k jest największą potęgą liczby 2 mniejszą od j. Czy metoda byłaby nadal poprawna, gdyby jako k brać: największą potęgę liczby 3 mniejszą od j? W przypadku pozytywnej odpowiedzi oszacuj, jak zmieniłby się oczekiwany koszt metody.
(Przypomnijmy, że metoda Pollarda generuje x-y za pomocą „pseudolosowej funkcji": $x_{j+1} = x_j^2+1 \bmod n$ i oblicza NWD(x_j-x_k, n) dla k wybranego jak wyżej, w nadziei, że $x_j = x_k \bmod p$ dla pewnego $p|n$, ale $x_j \neq x_k \bmod n$.)

4. Rozważ schemat szyfrowania ElGamala za pomocą bezpiecznego urządzenia, w którym wartość k nie jest losowana, lecz jest wyliczana jako $H(z)$, gdzie H jest funkcją hashującą, a z jest ciągiem znaków wprowadzanych przez szyfrującego:
$y_1 := g^{H(m)} \bmod p, y_2 = m \cdot \beta^{H(m)} \bmod p$, gdzie $\beta = g^x \bmod p$.
Czy taki schemat jest bezpieczny?

5. Załóżmy, że atakujący może dodać (modulo 2^{32}) wybraną liczbę do zawartości R_{15} w algorytmie DES. Jak zmodyfikować kryptoanalizę różnicową, aby zmontować skuteczny atak przeciwko DES-owi?

6. Jaś zamienił w algorytmie Rijndael operacje z udziałem klucza i operacje dokonywane w kolumnie. Następnie stwierdził, że modyfikacja jest tak dobra, że można zredukować liczbę rund algorytmu do dwóch. Co sądzisz o takiej modyfikacji w kontekście niezmienionej operacji ShiftRow?

7. Dysponujemy implementacją jednokierunkowej bezkolizyjnej funkcji hashującej f o wynikach długości 160 bitów. Dla pewnych celów pragniemy mieć taką funkcję, lecz o wynikach 159-bitowych. Czy usunięcie ostatniego bitu z wartości funkcji f rozwiązuje nasz problem?

8. Hashowanie oparte na problemie dyskretnego logarytmu możemy spróbować oprzeć na trzech liczbach rzędu q:
$$H(x, y, z) := \alpha^x \cdot \beta^y \cdot \gamma^z \bmod p$$
Czy będzie to bezpieczne?

9. Alicja uwierzytelniła się wobec Boba przy pomocy protokołu z wiedzą zerową. Bob wszystko rejestrował i zapis przedstawił Rafałowi, aby udowodnić, że rozmawiał z Alicją. Czy Rafał powinien zaakceptować ten dowód?

10. Przedstawić możliwie najprostszy algorytm przekazania klucza przez Alicję Bobowi, tak aby był on odporny na atak przez replay.