Bezpieczeństwo komputerowe

semestr letni 2023/24

Lista nr 5

(laboratorium)

Terminy oddania: przed 25.05.2024

Zadanie 1. RC4 (5 pkt). Napisz w wybranym języku implementację RC4 (zakładamy, że wiadomości zawierają tylko znaki ASCII, implementacja jest zgodna z pierwotną specyfikacją, czyli nie ma żadnych IV). Wygeneruj pewną liczbę kryptogramów przy użyciu klucza k oraz pewną liczbę kryptogramów przy użyciu klucza $k' \neq k$. Sprawdź poprawność procedury deszyfrowania.

Zadanie 2. Wykrywanie użycia tego samego klucza (5 pkt). Napisz funkcję pobierającą jako input dwa kryptogramy C oraz C' (powstałe jako rezultat szyfrowania wiadomości za pomocą twojej implementacji RC4), która pozwala stwierdzić, czy do obliczenia C i C' użyto tego same klucza. Jeżeli samodzielnie nie wpadniesz na pomysł jak to sprawdzić, szukaj wskazówki w pracy https://eprint.iacr.org/2005/007.pdf

Zadanie 3. Atak (5pkt). Przy użyciu twojej implementacji RC4 i tego samego klucza przygotuj pewną liczbę kryptogramów numerów kont bankowych z 5 polskich banków (wybrane przez Ciebie). Pamiętaj, że numer konta bankowego posiada format CCAAAAAAAABBBBBBBBBBBBBB, gdzie:

- CC (2 cyfry) – to suma kontrolna
- AAAAAAAA (8 cyfr) – to tzw. numer rozliczeniowy banku
- BBBBBBBBBBBBBB (16 cyfr) – to numer rachunku klienta

szczegóły znajdziesz w Zarządzeniu nr 7/2017 Prezesa NBP (dostępne https://ewib.nbp.pl/faces/pages/wazneInformacje.xhtml)

Wykorzystując fakt, że zastosowano te same klucze do RC4 oraz format szyfrowanych wiadomości, przeanalizuj XORy par kryptogramów w celu odgadnięcia zaszyfrowanych numerów kont (bez znajomości klucza). Napisz program łamiący RC4 przy tych założeniach. Ile kryptogramów numerów rachunków potrzebuje do działania?