Kryptografia i kryptoanaliza

Laboratorium 6

Michał Łaskawski

Zadanie 1

Dokonać implementacji kryptosystemu strumieniowego, którego strumień klucza k generowany jest przy pomocy rejestrów przesuwnych X, Y oraz Z, gdzie: $x_{i+3} = x_i \oplus x_{i+1}$, $y_{i+4} = y_i \oplus y_{i+3}$, $z_{i+5} = z_i \oplus z_{i+2}$, natomiast i-ty bit strumienia klucza określony jest funkcją łączącą: $k_i = f(x_i, y_i, z_i) = x_i y_i \oplus y_i z_i \oplus z_i$.

Kryptosystem taki powinien mieć zdefiniowane metody:

- szyfrowania danych pobranych z pliku oraz zapisu szyfrogramu do wskazanego pliku,
- jak również odszyfrowania szyfrogramu i zapisania wyniku do określonego pliku.

Uwagi:

1. Jeżeli:
   - $\mathcal{L}_X$ jest długością cyklu generowanego przez rejestr przesuwny X, a $\mathcal{L}_Y$ i $\mathcal{L}_Z$ są długościami cyklów rejestrów Y oraz Z, to strumień klucza wygenerowany przez podany kryptosystem będzie miał długość: $\mathrm{lcm}(\mathcal{L}_X, \mathcal{L}_Y, \mathcal{L}_Z)$, gdzie lcm to najmniejsza wspólna wielokrotność.
   - Dla Zdefiniowanego w ramach zadania kryptosystemu, długość cyklu generatora klucza będzie wynosić: $\mathcal{L}_X = 7$, $\mathcal{L}_Y = 15$ i $\mathcal{L}_Z = 31$ bitów. Zatem ostatecznie, długość cyklu będzie wynosić 3255 bitów, pod warunkiem, że początkowym wypełnieniem żadnego z rejestrów nie jest wektor zerowy.
2. Z konstrukcji generatora klucza, wynika iż do zainicjowania pracy kryptosystemu, konieczny jest 12 bitowy klucz, określający początkowe wypełnienia rejestrów. Jeżeli początkowe wypełnienia rejestrów wynoszą: X: 011, Y: 0101, Z: 11100, to pierwsze 31 bitów generatora powinno być następujące:

Tabela 1: Bity rejestru i strumień klucza

Bity	i = 0, 1, 2, . . . , 29, 30
x_i	0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1
y_i	0 1 0 1 1 0 0 1 0 0 0 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1 1 1 0
z_i	1 1 1 0 0 0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1 1 0 0 1 1
k_i	1 1 1 1 0 0 1 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 1 0 1 0 1 1

Zadanie 2

Dokonać *ataku korelacyjnego* na zbudowany w ramach pierwszego zadania kryptosystem, przyjmując iż znany jest szyfrogram i odpowiadające mu dane jawne. Zadaniem jest odzyskanie klucza a następnie początkowych wypełnień rejestrów generatora strumienia klucza kryptosystemu.

Uwagi:

1. Zgodnie z zasadą Kreckhoff'a, do dalszej pracy należy przyjąć, iż atakujący zna:
   - funkcje sprzężenia zwrotnego LFSR,
   - oraz nieliniową funkcję bool'owską f.

   Atakujący nie zna klucza (początkowych wypełnień LFSR), którą zaszyfrowano wiadomość.
2. Tabela prawdy funkcji logicznej f ujawnia, iż: $f(x, y, z) = x$ oraz $f(x, y, z) = z$ zachodzi z prawdopodobieństwem równym $\frac{3}{4}$.

Tabela 2: Tabela prawdy dla zdefiniowanej funkcji f

x	y	z	xy	yz	f
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	0	0	0
1	0	1	0	0	1
1	1	0	1	0	1
1	1	1	1	1	1

Atakujący może wykorzystać ten fakt do odzyskania początkowych wypełnień rejestrów X oraz Z generatora strumienia klucza. Można tego dokonać w następujący sposób:

- Wygenerować zbiór wszystkich możliwych permutacji początkowego wypełnienia wybranego rejestru (np. rejestru X).
- Dla każdej permutacji wygenerować strumień klucza (np. strumień składający się 31 bitów).
- Wybrać jedną z opcji:
  - Porównać bity odzyskanego strumienia klucza z bitami strumienia wygenerowanego przez analizowany rejestr dla danej permutacji. Jeżeli zachodzi zgodność pomiędzy tymi bitami z prawdopodobieństwem bliskim $\frac{3}{4}$, to można uznać, iż dane początkowe wypełnienie jest poszukiwanym wypełnieniem.
  - Alternatywnie można zbudować funkcję obliczającą współczynnik korelacji Pearsona (Algorytm 1) dla dwóch bitowych strumieni kluczy, odzyskanego strumienia klucza i wygenerowanego przez analizowany rejestr dla danej permutacji początkowej. Następnie wybrać taką permutację, dla której wartość bezwzględna różnicy pomiędzy jednością a obliczonym współczynnikiem korelacji będzie najmniejsza.

3. Przedstawionej techniki nie można zastosować do odzyskania początkowego wypełnienia rejestru Y. Wynika to z faktu, iż prawdopodobieństwo $f(x, y, z) = y$ wynosi dokładnie $\frac{1}{2}$. jednakże znając początkowe wypełnienia rejestrów X oraz Z można odzyskać początkowe wypełnienie rejestru Y stosując technikę *wyczerpującego wyszukiwania*.

Zadanie 3

Przeprowadzić atak korelacyjny na zbudowany w ramach pierwszego zadania kryptosystem, przyjmując iż znany jest szyfrogram i tylko fragment danych jawnych.

Zadanie 4

Przeprowadzić atak na zbudowany w ramach pierwszego zadania kryptosystem, przyjmując założenia z poprzedniego zadania, stosując jedynie technikę *wyczerpującego wyszukiwania*.

- Porównać wymagany do przeprowadzenia ataku nakład obliczeniowy z nakładem obliczeniowym wymaganym do przeprowadzenia ataku korelacyjnego.

Zadanie 5

Przedstawić wnioski dotyczące budowy nieliniowego generatora strumienia klucza dla kryptosystemu strumieniowego.

Współczynnik korelacji Pearsona

Algorithm 1 Wyznaczenie współczynnika korelacji Pearsona dla sekwencji bitowych

Require: $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ - wektory bitów (0 lub 1)
Ensure: ρ - współczynnik korelacji Pearsona

if $|\boldsymbol{x}| \neq |\boldsymbol{y}|$ **then**
    raise ValueError("Strumienie bitów muszą być tej samej długości")
end if
$n \leftarrow |\boldsymbol{x}|$
$\bar{x} \leftarrow \dfrac{1}{n}\sum_{i=1}^{n} x_i$
$\bar{y} \leftarrow \dfrac{1}{n}\sum_{i=1}^{n} y_i$
$\mathrm{cov}(X, Y) \leftarrow \dfrac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{n-1}$
$s_X \leftarrow \sqrt{\dfrac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}$
$s_Y \leftarrow \sqrt{\dfrac{\sum_{i=1}^{n}(y_i - \bar{y})^2}{n-1}}$
$\rho \leftarrow \dfrac{\mathrm{cov}(X, Y)}{s_X s_Y}$
return ρ