Kryptografia – laboratorium – ćwiczenie 1-2.
Badanie jakości S-bloku. Nieliniowość i kryterium SAC.

Przydatne definicje:

Waga Hamminga – hwt(x) – liczba jedynek w wektorze binarnym postaci $x \in \{0, 1\}^n$.

Odległość Hamminga – d(f,g) – odległość pomiędzy dwiema funkcjami boolowskimi f, g takimi, że $\{0, 1\}^n \rightarrow \{0, 1\}$, wskazująca liczbę argumentów, dla których funkcje te przyjmują różne wartości.

$$d(f, g) = \Sigma\, f(x) \bigoplus g(x)$$

Odległość funkcji od zbioru funkcji – δ(f) – najmniejsza wartość odległości Hamminga funkcji f od funkcji g, należącej do danego podzbioru n-argumentowanych funkcji boolowskich (X_n).

$$\delta(f) = min_{g \in X_n} d(f, g)$$

Nieliniowość funkcji – N_f – minimalna odległość funkcji f od zbioru wszystkich funkcji afinicznych.

Ścisłe kryterium lawinowości (SAC, ang. strict avalanche criterion) – własność bloku podstawień wskazująca, że zmiana jednego bitu na wejściu powinna skutkować „lawiną" zmian na wyjściu.

- Funkcja f: $\{0, 1\}^n \rightarrow \{0, 1\}$ spełnia kryterium lawinowości, jeśli średnio połowa bitów wyjścia ulega zmianie przy modyfikacji pojedynczego bitu wejścia.

- Funkcja f: $\{0, 1\}^n \rightarrow \{0, 1\}$ spełnia ścisłe kryterium lawinowości, wtedy i tylko wtedy, gdy funkcja $f(x) \oplus f(x \oplus \alpha)$ jest zbalansowana dla każdego wektora binarnego α.

Zadanie:

1. Otwórz plik sbox.sbx w edytorze plików binarnych i odczytaj zapisane w nim funkcje. Ile ich jest?
2. Sprawdź zbalansowanie każdej z funkcji. Czy cecha ta jest istotna z kryptograficznego punktu widzenia? Uzasadnij.
3. Określ nieliniowość badanych funkcji. W tym celu wygeneruj zbiór wszystkich 8-argumentowych funkcji afinicznych. Jaka jest liczność tego zbioru?
4. Sprawdź czy dla poszczególnych funkcji spełnione jest ścisłe kryterium lawinowości (SAC). Jaką wartość prawdopodobieństwa zmian na wyjściu udało się uzyskać dla całego bloku?
5. Sporządź krótkie sprawozdanie z zajęć. Powinno obejmować uzyskane wyniki: nieliniowość bloku, zbalansowanie tak/nie, SAC, opis metody generowania zbioru funkcji afinicznych, podsumowanie.