Bezpieczeństwo komputerowe

Lista nr 3 (A), 2-7 XI

Zadanie 1 (20 pkt) Przechwyciłaś/eś kilkanaście kryptogramów. Wiesz, że każdy z nich powstał jako rezultat szyfrowania wiadomości za pomocą szyfru strumieniowego. Co więcej, do szyfrowania każdej wiadomości wykorzystano ten sam klucz, czyli: $c_i = \mathsf{Enc}(\mathsf{k}, \mathsf{m_i}) = m_i \oplus G(k)$ dla $i = 1 \ldots l$, gdzie G jest generatorem bitów pseudolosowych, a k jest kluczem tajnym.

Napisz program (i umieść go na swoim koncie na github), który przyjmuje na wejściu l kryptogramów zaszyfrowanych za pomocą szyfru strumieniowego z tym samym kluczem. Na wyjściu program ma zwrócić teksty jawne.

Przeprowadź eksperymenty, aby określić skuteczność programu w zależności od:

- długości kryptogramów,
- liczby kryptogramów dla $l = 1, 2, 3, 4, \ldots$ (od jakiej wartości l, program zaczyna działać?)
- typu szyfru strumieniowego (Salsa20, Sosemanuk, ...)
- wykorzystanego kodowania znaków ASCII/UTF-8/ISO-8859-2?

Aby uzyskać przykładowe dane, wprowadź numer indeksu do formatki na stronie.