Zadanie 3. Tryby operacyjne ECB i CBC dla prostego szyfru blokowego. Wykorzystaj podane na wykładach algorytmy do rozwiązania poniższych zadań[1].

a) Skonstruuj prosty kaskadowy szyfr blokowy o bloku P długości 8 bit (1 B, tj. 1 znak ASCII) i kluczu K długości 8 bit (może być reprezentowany przez znak ASCII lub 2-cyfrową liczbę szesnastkową) złożony z dwóch etapów:

podstawienie dodanie klucza do reprezentacji ASCII znaku textu jawnego za pomocą operacji XOR:

$$B \leftarrow P \oplus K;$$

przestawienie obrót w lewo o 4 miejsca wyjścia 1. etapu o 4 bit (tj. zamiana miejscami cyfr szesnastkowych bloku):

$$C \leftarrow B \overset{4}{\hookleftarrow}.$$

Wyjściem szyfru jest blok C długości 8 bit. Zapisz ten blok jako 2-cyfrową liczbę szesnastkową[2]. (2 p.)

b) Utwórz dwa kryptogramy szyfrując dwoma różnymi wybranymi kluczami $0 \leqslant K < 256$ text jawny „`attack at down`" stosując tryb operacyjny ECB (tj. utwórz ciągi 2-cyfrowych liczb szesnastkowych odpowiedniej długości). (3 p.)

c) Utwórz dwa kryptogramy szyfrując dwoma różnymi wybranymi kluczami $0 \leqslant K < 256$ i dwoma różnymi wybranymi wektorami początkowymi $0 \leqslant IV < 256$ (tj. 8 bit czyli 1 B, może być reprezentowany jako 1 znak ASCII lub 2-cyfrowa liczba szesnastkowa) text jawny „`attack at down`" stosując tryb operacyjny CBC (tj. utwórz ciągi 2-cyfrowych liczb szesnastkowych odpowiedniej długości). (3 p.)

d) Powyższy szyfr w trybie operacyjnym ECB realizuje podstawienie proste na alfabecie $\mathbb{Z}_{256} = \{0, \ldots, 255\}$. Jakie jest prawdopodobieństwo, że oba kryptogramy otrzymane przy zastosowaniu trybu operacyjnego ECB odpowiadają temu samemu textowi jawnemu? Czy da się to samo stwierdzić w przypadku kryptogramów otrzymanych przy zastosowaniu trybu operacyjnego CBC? (2 p.)

---

[1] Rozwiąż zadanie za pomocą napisanych samodzielnie programów (języki: C/C++, Java, Python, Fortran, Bash) lub przez obliczenia na kartce. W przesłanym rozwiązaniu zamieść programy (w archiwum `.zip`) lub obliczenia (operacje arytmetyczne na liczbach naturalnych można wykonać za pomocą kalkulatora).

[2] Nie należy reprezentować wyjścia w postaci znaków ASCII, gdyż blok wyjściowy może zawierać reprezentację ASCII znaków niedrukowalnych.