

Kryptografia

Laboratorium nr 3

Stefan Sokołowski

Zadanie 1 (arytmetyka szesnastkowa):

Proszę z katalogu

stefan.info.pl/Dydaktyka/Krypto/Slajdy/Programy/HexArytm

pobrać programy **HexAryt.java** i **XOR.java** (drugi korzysta z pierwszego) i zobaczyć, w jaki sposób drugi z nich oblicza i wyświetla tabelkę XORowania. W podobny sposób wyświetlić sobie tabelki dodawania i mnożenia w układzie szesnastkowym.

Przy użyciu tych tabelek proszę wykonać (ręcznie na kartce) następujące działania:

(a)
$$\begin{array}{r} 7A23 \\ + BFF \\ \hline \dots \end{array}$$

(b)
$$\begin{array}{r} BD7 \\ \times 53 \\ \hline \dots \end{array}$$

(c)
$$\begin{array}{r} AE59 \\ \times 86C \\ \hline \dots \end{array}$$

Poprawność wyników proszę sprawdzić kalkulatorem.

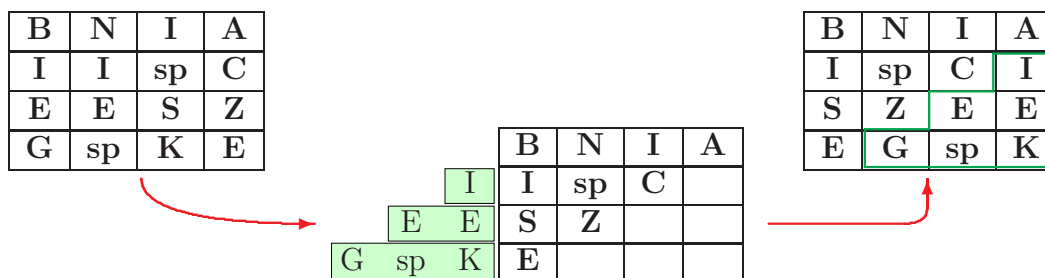
Zadanie 2 (*ShiftRows*):

Proszę napisać program, który

- wczytuje dowolny tekst,
- dzieli go na odcinki po 16 znaków (ew. dopełnia spacjami) i ustawia kolumnami w tablicach 4×4 ¹,
- w tablicach wykonuje cykliczne przesunięcia wierszy w lewo wg schematu *ShiftRows*²,
- tekst z tak zmienionych tablic odczytuje kolumnami i wyświetla;

oraz drugi program, który działa odwrotnie (przesuwa wiersze w prawo).

Poniższy rysunek ilustruje to szyfrowanie dla tekstu „BIEGNIE I SKACZE”:



Wynik: „BISEN ZGICE AIEK”.

¹Jak w stefan.info.pl/Dydaktyka/Krypto/Slajdy/03a.pdf str. 3.

²Por. stefan.info.pl/Dydaktyka/Krypto/Slajdy/03a.pdf str. 4.

Zadanie 3 (*MixColumns*):

Proszę wyliczyć iloczyn macierzy przez wektor wg zasad *MixColumns* jak w

stefan.info.pl/Dydaktyka/Krypto/Slajdy/03a.pdf str. 8

(ale proszę doliczyć do końca):

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 4E \\ 41 \\ 20 \\ 55 \end{bmatrix} = ?$$

Zadanie 4 (*SubBytes*):

Krótki tekstik zapisałem szesnastkowymi kodami ASCII jego znaków, a następnie do tych kodów zastosowałem zastąpienie *S-box* i otrzymałem taki ciąg liczb szesnastkowych:

5B F9 A8 71 B7 7F A8 9F F9 7F 9D FD

Proszę zastosować do niego odwrotne zastąpienie *S-box*³ a następnie otrzymane kody ASCII zamienić na czytelne znaki.

Zadanie 5 (domowe specjalne):

Proszę napisać

- (a) program realizujący specjalne mnożenie liczb szesnastkowych zdefiniowane w stefan.info.pl/Dydaktyka/Krypto/Slajdy/03a.pdf str. 7,
- (b) program (wykorzystujący ten z pkt.(a)) wykonujący mnożenie macierzy 4×4 liczb szesnastkowych przez ich wektory długości 4 (jak w tym samym wykładzie na str. 8).

Uwaga:

Pierwszej osobie, która przyśle mi (na s.sokolowski@ans-elblag.pl) poprawne rozwiązanie tego zadania, przysługują punkty do zaliczenia laboratorium/ćwiczeń. Liczba tych punktów zależy od oryginalności i elegancji rozwiązania. W mailu proszę koniecznie podać swoje **nazwisko, numer zajęć i numer zadania**.

³Tabela podana w stefan.info.pl/Dydaktyka/Krypto/Slajdy/03a.pdf str. 11.