Zadanie 5

Rozważmy zmodyfikowany szyfr Cezara, w którym kluczem jest pewne słowo dowolnej długości, a proces szyfrowania wiadomości przebiega w następujący sposób. Dla wiadomości długości n, postaci $W = w_1 w_2 \dots w_n$ oraz klucza długości m, postaci $K = k_1 k_2 \dots k_m$, każdą literę wiadomości i klucza zamieniamy na odpowiadający element w grupie multiplikatywnej ciała $GF(3^3) \cong \mathbb{Z}_3/x^3 + 2x^2 + 1$, czyli mamy $a \mapsto 1$, $b \mapsto 2$, $c \mapsto x$, $\dots$ $z \mapsto 2x^2 + 2x + 2$. Następnie każdy znak z wiadomości w_i mnożymy przez odpowiedni znak klucza $k_{i \bmod m}$ otrzymując szyfrogram postaci: $w_1 \cdot k_1, w_2 \cdot k_2, \dots w_n \cdot k_{n \bmod m}$.

Przy pomocy powyższego szyfru grupa matematyków zaszyfrowała tajną wiadomość. Jednak została ona przechwycona przez agenta Bałwana, który odczytał szyfrogram o treści "mglvwgxgyweglqezf". Dodatkowo agent Bałwan dokonał podsłuchu przesyłu dwóch innych wiadomości wraz z ich szyfrogramami, jednak w wyniku zakłóceń z pierwszej wiadomości otrzymał jedynie początek "fish" z szyfrogramem "jfnv", a z drugiej tylko część znaków "h___y_o___op__kny__h_ma_" razem z wybrakowanym szyfrogramem "gg_wd_w_x___u_fzfil__gey". Czy dasz radę odszyfrować tajną wiadomość matematyków oraz ich klucz?

Podpowiedzi :)

- Na pewno pomocna będzie poniższa tabela generatora grupy multiplikatywnej ciała $GF(3^3)$.

x^i	element grupy
x^1	x
x^2	x^2
x^3	x^2+2
x^4	x^2+2x+2
x^5	$2x+2$
x^6	$2x^2+2x$
x^7	x^2+1
x^8	x^2+x+2
x^9	$2x^2+2x+2$
x^{10}	x^2+2x+1
x^{11}	$x+2$
x^{12}	x^2+2x
x^{13}	2
x^{14}	$2x$
x^{15}	$2x^2$
x^{16}	$2x^2+1$
x^{17}	$2x^2+x+1$
x^{18}	$x+1$
x^{19}	x^2+x
x^{20}	$2x^2+2$
x^{21}	$2x^2+2x+1$
x^{22}	x^2+x+1
x^{23}	$2x^2+x+2$
x^{24}	$2x+1$
x^{25}	$2x^2+x$
x^0	1

Tabela 1: Tabela generatora grupy multiplikatywnej ciała $GF(3^3)$.

- W razie pojawienia się problemów z odnalezieniem klucza możesz spró-

bować wykorzystać socjotechniki w celu zdobycia informacji na temat jego długości.

- Flaga jest w postaci "klucz_tajna wiadomość".