

Obok niesławnego Kuby Rozpruwacza jednym z najbardziej znanych nieuchwytnych, seryjnych morderców jest niewątpliwie postać o pseudonimie Zodiak. Jego posępna aktywność miała miejsce na przełomie lat 60. i 70. XX wieku w okolicach San Francisco. Duży wpływ na zakorzenienie się Zodiaka w świadomości publicznej miały listy, które wysyłał do lokalnych gazet. Oprócz gróźb kierowanych do kalifornijskiej społeczności w niektórych listach znajdowały się zaszyfrowane wiadomości. Morderca sugerował, że ich rozszyfrowanie pomoże władzom ustalić jego tożsamość. Znane są cztery kryptogramy Zodiaka – Z408, Z340, Z13 i Z32 (liczby oznaczają, z ilu symboli składają się poszczególne wiadomości).

Zaszyfrowane informacje składające się na Z408 zostały opublikowane 31 lipca 1969 roku w trzech lokalnych kalifornijskich gazetach. Niewiele ponad tydzień od publikacji szyfr został złamany przez małżeństwo Betty i Donalda Hardenów, którzy później stwierdzili, że nad swoim rozwiązaniem pracowali w sumie około 20 godzin. Okazało się, że w pierwszym szyfrogramie Zodiak zastosował *homofoniczny szyfr podstawieniowy*.

Szyfry podstawieniowe polegają na zamianie każdego symbolu wiadomości jawnej na inny symbol, zgodnie z ustaloną zasadą podstawiania. Na przykład, stosując podstawienie

$$A \rightarrow J, E \rightarrow +, K \rightarrow /, M \rightarrow \rho, T \rightarrow \bullet, Y \rightarrow \square,$$

możemy zaszyfrować słowo MATEMATYKA jako $\rho J \bullet + \rho J \bullet \square / J$. Oczywiście alfabet kryptogramu nie musi się różnić od alfabetu wiadomości jawnej – klasycznym przykładem prostego szyfru podstawieniowego jest tzw. *szyfr Cezara*.

W szyfrze Cezara każda litera alfabetu łacińskiego (za wyjątkiem trzech ostatnich) zastępowana jest literą znajdującą się trzy pozycje dalej w alfabecie, natomiast ostatnie trzy litery – odpowiadającymi im trzema pierwszymi literami. SURVWH.

Proste szyfry podstawieniowe cechują się tym, że można je bardzo łatwo złamać – wystarczy przeprowadzić analizę częstości występowania poszczególnych znaków. Przykładowo: najczęściej występującą literą w tekstach w języku polskim jest A, z częstotliwością wystąpień 8,91%. Jak widać na powyższym przykładzie, faktycznie najczęściej występujący znak J odpowiada literze A (mimo iż przykład sam w sobie nie jest reprezentatywny pod tym względem; im dłuższa jest zaszyfrowana wiadomość, tym dokładniej jej rozkład częstości występowania znaków odpowiada rozkładowi otrzymanemu z dowolnego równie długiego tekstu zapisanego w tym języku).

Wariantem odpornym na przedstawioną wyżej elementarną analizę częstości jest szyfr homofoniczny. W tej wersji poszczególne znaki mogą być szyfrowane na kilka sposobów w zależności od tego, jak często występują w tekstach w danym języku. I tak w szyfrze Zodiaka rzadko występującej w języku angielskim literze K (1,1%) przydzielono tylko jeden symbol $/$, natomiast najczęściej występującej literze E (11,16%) – aż siedem symboli: E, N, W, Z, 9, +, \odot .

Hardenowie skupili się na wyszukiwaniu par identycznych symboli. Zauważyli, że w Z408 występują dwie pary $\square\square$ oraz para $\bullet\bullet$. Najczęściej występującą parą w języku angielskim jest LL, więc założyli, że każdy z symboli \square oraz \bullet odpowiada literze L. Następnie, biorąc pod uwagę kontekst sytuacji, zaczęli wyszukiwać w szyfrogramie czterosymbolowych segmentów, które mogłyby odpowiadać słowu KILL. W ten sposób udało im się ustalić przyporządkowania $K \rightarrow /$, $I \rightarrow \{P, U, \Delta\}$ oraz $L \rightarrow B$. Mając częściowo rozszyfrowany tekst, Betty (wiedziona intuicją) odgadła, że wiadomość zaczyna się od słów ILIKEKILLING. Po odszyfrowaniu tego fragmentu Hardenowie mogli już bardzo łatwo ustalić pozostałe przyporządkowania. Wiadomość okazała się opisem okrutnych motywacji kierujących mordercą.

Trzy miesiące później, 8 listopada, został opublikowany kolejny kryptogram Zodiaka – Z340. Pierwsze propozycje „złamania” szyfru przedstawiono niedługo po publikacji, jednak ostatecznie przez ponad pół wieku nikomu nie udało się znaleźć przekonującego rozwiązania. Do najpopularniejszych błędnych rozwiązań Z340 należy rozwiązanie zaprezentowane przez Roberta Graysmitha.

Robert Graysmith jest autorem książki, która posłużyła za podstawę scenariusza filmu fabularnego *Zodiak* z 2007 roku w reżyserii Davida Finchera.

Fundamentalną wadą tego rozwiązania jest fakt, że Graysmith arbitralnie przepermutował 86% symboli znajdujących się w wiadomości w taki sposób, aby ich kolejność pasowała do obranej przez niego metody podstawiania (dodatkowo całkowicie zignorował niektóre z symboli). Słabość tej metody stanowi fakt, że może ona wygenerować olbrzymią liczbę różnych rozwiązań (wystarczy dokonać innych permutacji). Graysmith przez jakiś czas poprawiał swoje rozwiązanie, ale nigdy nie zrezygnował z wątpliwych metod deszyfracji.

Zodiak najprawdopodobniej postanowił usprawnić metodę szyfrowania wiadomości, gdy uświadomił sobie, jak niewiele czasu wymagało złamanie Z408. Ze statystycznego punktu widzenia szybko stało się jasne, że Z340 został zaszyfrowany co najmniej dwuetapowo. W międzyczasie belgijski programista Jarl van Eycke stworzył program *AZdecrypt*, służący do łamania homofonicznych szyfrów podstawieniowych (głównym elementem deszyfracji jest analiza częstości występowania identycznych par symboli). Zaszyfrowaną informację Z408 program van Eycke’a jest w stanie złamać w ułamku sekundy, nie radzi sobie jednak z szyfrem Z340, co dodatkowo wspiera tezę, że szyfr jest bardziej skomplikowany od swojego poprzednika. Jak się ostatecznie okazało, Zodiak użył homofonicznego szyfru podstawieniowego oraz pewnego wariantu *szyfru przestawieniowego*.

Szyfrowanie przestawieniowe polega na zmianie kolejności występujących w tekście symboli, zgodnie z precyzyjnie ustaloną zasadą. Jednym z najprostszych modeli szyfru przestawieniowego jest zapisanie tekstu

jawnego w prostokącie (np. od góry do dołu, od lewej do prawej) i odczytanie go względem innej orientacji (np. od lewej do prawej, od góry do dołu). Rozważmy tekst jawny **PROSTYSZYFRPRZESTAWIENIOWY** i zapiszmy go zgodnie z sugerowaną w nawiasie zasadą, w prostokącie o wysokości 4:

P T Y R T E W
R Y F Z A N Y
O S R E W I
S Z P S I O

Zapisując otrzymany tekst od lewej do prawej i od góry do dołu, otrzymujemy szyfrogram **PTYRTEWRYFZANYOSREWISZPSIO**. Szyfry przestawieniowe stosowane samodzielnie są niezwykle proste do złamania, o czym można się przekonać, rozszyfrowując poniższą wiadomość:

PCRKIOOANBLILCEEICMEŠTMMRNIZYEELRCACHSI.

Jednak zastosowanie pewnej modyfikacji szyfru przestawieniowego w **Z340** niezwykle skomplikowało zadanie osobom próbującym odtworzyć tekst jawny.

W 2020 roku pandemia COVID-19 zapewniła australijskiemu matematykowi Samowi Blake'owi trochę wolnego czasu od dotychczasowych obowiązków na Uniwersytecie w Melbourne. Blake zainteresował się też amerykańskiego informatyka Davida Oranchaka, który podczas jednego z wykładów zasugerował, że być może **Z340** jest nie tylko szyfrem podstawieniowym, ale również przestawieniowym. Przypuszczenie to wywodziło się z analizy statystycznej występowania par symboli przy pewnych rearanżacjach układu tekstu szyfrogramu. Matematyk skontaktował się z Oranchakiem i wspólnie zaczęli analizować **Z340** pod kątem szyfru przestawieniowego. Ich metoda polegała na przestawianiu symboli zawartych w **Z340** i analizie otrzymanych szyfrogramów za pomocą *AZdecrypt*. Gdy to podejście nie przyniosło rezultatu, badacze postanowili dzielić **Z340** na mniejsze części i analizować je osobno. Oryginalnie **Z340** został zapisany w prostokącie 20×17 . Po żmudnych obliczeniach, przy podzieleniu tekstu na trzy prostokąty 9×17 , 9×17 i 2×17 i zastosowaniu opisanego poniżej przestawienia, udało im się rozszyfrować pierwszych 9 linijek wiadomości. Kolejność zapisu symboli przez Zodiaka w tym prostokącie przypomina ruch skoczka na szachownicy – pierwszy symbol został zapisany w lewym górnym rogu, a każdy następny o jeden wiersz niżej i dwie kolumny dalej (z modularnym przejściem przez krawędzie prostokąta):

1	10	19	28	37	46	55	64	73	82	91	100	109	118	127	136	145
137	146	2	11	20	29	38	47	56	65	74	83	92	101	110	119	128
120	129	138	147	3	12	21	30	39	48	57	66	75	84	93	102	111
103	112	121	130	139	148	4	13	22	31	40	49	58	67	76	85	94
86	95	104	113	122	131	140	149	5	14	23	32	41	50	59	68	77
69	78	87	96	105	114	123	132	141	150	6	15	24	33	42	51	60
52	61	70	79	88	97	106	115	124	133	142	151	7	16	25	34	43
35	44	53	62	71	80	89	98	107	116	125	134	143	152	8	17	26
18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	9

Jednak zastosowanie otrzymanego w tym prostokącie homofonicznego klucza do pozostałej części tekstu nie przynosiło rezultatów. Blake i Oranchak postanowili skontaktować się z van Eyce'em i przedstawić mu swoje częściowe rozwiązanie. Twórca *AZdecrypt* szybko odkrył, jak dwie drobne modyfikacje „ruchu skoczka szachowego” pozwolą rozszyfrować wiadomość ukrytą w drugim prostokącie. Natomiast w ostatnim – najkrótszym – fragmencie szyfrogramu wystarczyło niektóre otrzymane słowa odczytać od tyłu – zachęcamy do samodzielnego przeprowadzenia tego etapu (w rozwiązaniu znajduje się popełniony przez Zodiaka błąd ortograficzny):

EFIL WILL EB NA EASY ENO NI ECIDARAP DEATH

Ostatecznie okazało się, że tekst jawny **Z340** – podobnie jak **Z408** – nie zawiera żadnych bezpośrednich wskazówek dotyczących tożsamości mordercy.

Ostatnie dwa szyfrogramy Zodiaka pozostają wciąż nierozwiązane. Niestety są one zbyt krótkie, aby można było poddać je metodom kryptoanalitycznym. Rozwiązanie każdego z nich wymagałoby wiarygodnego uzasadnienia przyjętego klucza deszyfracji. W jednym ze swoich kolejnych listów Zodiak zawarł bezpośrednią wskazówkę do rozszyfrowania **Z32**, jednak do dzisiaj nie została ona przez nikogo przekonująco zinterpretowana.

Tekst jawny zawiera polskie tytuły książek składających się na pewną trylogię sci-fi (pierwszy tom zawiera intrygujący wątek matematyczny).

David Oranchak od wielu lat zajmuje się kryptologicznymi aspektami działalności Zodiaka. Między innymi jest autorem serii filmów poświęconych tej tematyce. Można je znaleźć na YouTube pod wspólną nazwą *Let's crack Zodiac*. Polecam je każdemu zainteresowanemu zagadnieniami omawianymi w niniejszym artykule.



Wskazówki do zadań z artykułu Blokowe cechy podzielności

1. Możesz zbadać, kiedy taka liczba dzieli się przez 9, a kiedy przez 11.
2. Kluczowe okaże się, że 1001 jest wielokrotnością liczby 7.
3. Ile cyfr może mieć taka liczba?