Rozwiązanie zadania F 1071.
Podczas jazdy ze stałą prędkością v na odcinku drogi l pokonanie oporu powietrza związane jest z wykonaniem pracy $W = \frac{1}{2}C\rho Sv^2 l$. Energia kinetyczna samochodu wynosi: $E_k = \frac{1}{2}mv^2$. Praca W zrówna się z energią E_k po przejechaniu odcinka drogi

$$l = \frac{m}{CS\rho}.$$

Dla przyjętych danych liczbowych $l \approx 1670$ m. Podczas rozpędzania ze stałym przyspieszeniem do prędkości 100 km/h ($v \approx 28$ m/s) osiąganej po czasie 10 s samochód pokonuje około 140 m.

Alternatywy dla OTW?

OTW jest dobrze sprawdzającym się modelem grawitacji, który doskonale zgadza się z precyzyjnymi badaniami w obrębie Układu Słonecznego, w układach podwójnych pulsarów, z soczewkowaniem grawitacyjnym czy badaniami kosmologicznymi. Należy jednak pamiętać, że obserwacje te dotyczą reżimu słabych pól grawitacyjnych. Każda nowo zaproponowana teoria musi być zgodna ze wszystkimi testami, jakie przeszła do tej pory OTW. Omówione powyżej istniejące otwarte problemy OTW są dobrą motywacją dla środowiska fizyków teoretyków do poważnego zajęcia się zmodyfikowanymi teoriami grawitacji. Obecnie istnieje wiele alternatyw dla OTW, a codziennie pojawiają się nowe prace prezentujące różne zmodyfikowane teorie mogące wytłumaczyć obserwacje, z którymi OTW ma problemy. Teoretycznie możliwości modyfikacji grawitacji jest wiele, ale to zgodność z danymi obserwacyjnymi jest ostatecznym czynnikiem decydującym. Oczekuje się, że rosnące możliwości technologiczne pozwalające na badanie wyższych energii i większych odległości w tym ogromnym Wszechświecie dadzą nam jakieś wskazówki dotyczące zachowania praw grawitacji.

Szyfr Lorenza i jego złamanie (1)

*Bartosz KLIN**

* Uniwersytet Oksfordzki

Chyba wszyscy słyszeli o niemieckiej maszynie szyfrującej Enigma z czasów II wojny światowej. Historia złamania jej szyfru jest nam szczególnie bliska ze względu na ważną rolę, jaką odegrali w niej polscy kryptologowie. Pamiętamy, jak zespół matematyków z wojskowego Biura Szyfrów złamał kod Enigmy na długo przed wojną, a na krótko przed jej wybuchem przekazał całą swoją wiedzę angielskim kryptologom, którzy w ośrodku w Bletchley Park, z udziałem genialnego Alana Turinga, łamali kolejno udoskonalane wersje maszyny. Ta pobudzająca wyobraźnię historia doczekała się – i słusznie! – licznych opisów w artykułach, książkach i filmach.

Jednak tysiące ludzi pracujących w centrum Bletchley Park i innych powiązanych z nim ośrodkach nie zajmowały się wyłącznie łamaniem szyfru Enigmy. Spośród kilkunastu innych szyfrów niemieckich badanych przez Anglików szczególnie ważny był ten oparty na maszynie szyfrującej Lorenz SZ40/42. Historia złamania tego szyfru jest o wiele mniej znana, a pod pewnymi względami bardziej imponująca niż historia Enigmy.

Po pierwsze, komunikaty zakodowane szyfrem Lorenza często miały o wiele większe znaczenie wywiadowcze. Armia niemiecka używała tysięcy egzemplarzy Enigmy na wszystkich szczeblach dowodzenia, ale większość komunikatów szyfrowanych za ich pomocą miała znaczenie co najwyżej taktyczne. Tymczasem maszyny Lorenza, uważane przez Niemców za bezpieczniejsze, były używane tylko w sztabach armii do przekazywania najważniejszych informacji i rozkazów o strategicznym znaczeniu. Szyfrowane nimi komunikaty często były długie, szczegółowe i pełne bardzo cennych informacji, a rozkazy niekiedy podpisywane przez samego Adolfa Hitlera.

Po drugie, polscy, a później angielscy kryptologowie, przystępując do łamania szyfru Enigmy, wiedzieli całkiem sporo o jej konstrukcji i zasadzie działania. Komercyjne, uproszczone wersje maszyny były dostępne na rynku na długo przed wojną, a wywiady polski i francuski miały dostęp także do egzemplarzy i opisów wersji wojskowych. To nie umniejsza znaczenia ogromnej pracy matematycznej, jaka była konieczna do złamania szyfru Enigmy, ale jednak dało solidny punkt startowy dla tej pracy. Tymczasem żaden egzemplarz maszyny Lorenza, ani żaden jej opis, aż do końca wojny nie wpadł w ręce aliantów. Strukturę tej maszyny odgadnięto, a sam szyfr złamano, posługując się wyłącznie nasłuchem radiowym i matematyką.

W chwili wybuchu wojny Enigma, opatentowana i wprowadzona na rynek jeszcze w latach dwudziestych, była już trochę przestarzałą konstrukcją. Była też dość niewygodna w użyciu: sama maszyna jedynie szyfrowała komunikat, ale nigdzie

Maszyna Lorenz SZ40

go nie wysyłała. Operator wpisywał kolejne znaki komunikatu na klawiaturze maszyny. Po każdym naciśnięciu klawisza na maszynie zapalała się lampka odpowiadająca kolejnej literze szyfrogramu, a operator pracowicie notował te litery. Następnie wysyłał cały szyfrogram przez radio, posługując się alfabetem Morse'a. Odbiorca komunikatu wykonywał te same czynności w odwrotnej kolejności. Było to niewygodne i czasochłonne, szczególnie przy nadawaniu długich komunikatów.

Maszynę Lorenz SZ40 i jej ulepszoną wersję SZ42 zaprojektowano już podczas wojny wyłącznie na potrzeby armii niemieckiej. Było to urządzenie o wiele nowocześniejsze i wygodniejsze. Przede wszystkim maszyna mogła nie tylko szyfrować i odszyfrowywać komunikaty, ale od razu nadawała je i odbierała drogą radiową, co znacznie upraszczało pracę operatora. Szyfrogramy nie były nadawane przestarzałym alfabetem Morse'a dostosowanym do ręcznych XIX-wiecznych telegrafów, ale tak zwanym międzynarodowym alfabetem telegraficznym ITA2, który od lat dwudziestych stanowił powszechnie przyjęty standard w komunikacji radiowej za pomocą dalekopisów.

W alfabecie ITA2, który można uznać za daleki pierwowzór znanego nam współcześnie kodu ASCII, każda litera jest kodowana za pomocą pięciu bitów, tak jak w poniższej tabeli.

Symbol ● oznacza obecność, a ○ – brak sygnału. Znaki były interpretowane w dwóch trybach: zwykłym i numerycznym, a do przełączania między nimi służyły znaki specjalne ⇑ i ⇓. Znaki przestankowe występowały tylko w trybie numerycznym.

Znaki ↵ i → to znaki końca linii, dziś zwykle oznaczane `CR` i `LF`. „Pusty" znak / nie miał przypisanej żadnej funkcji.

–	?	:		3	!	&	£	8		(	)	.	,	9	0	1	4	′	5	7	=	2		6	+	_	↵	→		⇓	/
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	↵	→	⇑		/
●	●	○	●	●	●	○	○	○	●	●	○	○	○	○	○	●	○	●	○	●	○	●	●	●	●	○	○	○	●	●	○
●	○	●	○	○	○	●	○	●	●	●	●	○	○	○	●	●	●	○	○	●	●	●	○	○	○	○	○	●	●	●	○
○	○	●	○	○	●	○	●	●	○	●	○	●	●	○	●	●	○	●	○	●	●	○	●	●	○	●	○	○	○	●	○
○	●	●	●	○	●	●	○	○	●	●	○	●	●	●	○	○	●	○	○	○	●	○	●	○	○	○	●	○	●	●	○
○	●	○	○	○	○	●	●	○	○	○	●	●	○	●	●	●	○	○	●	○	●	●	●	●	●	○	○	○	●	●	○

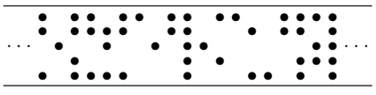
Przykładowo, komunikat

`W 2023 – DELTA!`

był kodowany jako

`W_⇑WPWE_A⇓_DELTA⇑F⇓`

Na perforowanej taśmie telegraficznej, gdzie perforacje odpowiadały symbolom ●, wyglądało to tak:



To oczywiście jeszcze nie jest żaden szyfr. Alfabet telegraficzny był powszechnie przyjętym standardem i zwykły dalekopis potrafił nadawać i odbierać komunikaty zakodowane w ten sposób.

Szyfr Vernama

Ogólną metodę szyfrowania tekstów zapisanych alfabetem telegraficznym obmyślił i opatentował jeszcze w 1919 roku amerykański inżynier Gilbert S. Vernam (1890–1960). Opiera się ona na prostej operacji dodawania bitów:

$$\circ + \circ = \circ \qquad \circ + \bullet = \bullet \qquad \bullet + \circ = \bullet \qquad \bullet + \bullet = \circ$$

Jest to powszechnie stosowana w informatyce i logice operacja, znana jako XOR, alternatywa rozłączna czy też dodawanie modulo 2. Można ją w oczywisty sposób rozszerzyć do dodawania znaków alfabetu telegraficznego „po współrzędnych", na przykład:

$$\mathtt{B} + \mathtt{K} = \begin{matrix}\bullet & \bullet & \circ\\ \circ & \bullet & \bullet\\ \bullet & \bullet & \circ\\ \bullet & \circ & \bullet\end{matrix} + \begin{matrix}\bullet & \circ & \bullet\\ \bullet & \bullet & \circ\\ \bullet & \bullet & \circ\\ \circ & \bullet & \bullet\end{matrix} = \begin{matrix}\bullet & \bullet & \circ\\ \circ & \bullet & \bullet\\ \circ & \circ & \circ\\ \bullet & \circ & \bullet\end{matrix} = \mathtt{P}$$

+	A	B	C	D	E	F	G	H	I	···
A	/	G	F	R	→	C	B	Q	S	···
B	G	/	Q	T	O	H	A	F	⇓	···
C	F	Q	/	U	K	A	H	G	↵	···
D	R	T	U	/	↵	_	W	X	K	···
E	→	O	K	↵	/	N	⇑	Y	U	···
F	C	H	A	_	N	/	Q	B	J	···
G	B	A	H	W	⇑	Q	/	C	M	···
H	Q	F	G	X	Y	B	C	/	L	···
I	S	⇓	↵	K	U	J	M	L	/	···
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Powstaje w ten sposób „tabliczka dodawania" liter (patrz margines), którą każdy kryptolog w Bletchley Park musiał znać na pamięć nie gorzej niż szkolną tabliczkę mnożenia.

Tę operację można dalej rozszerzyć do dodawania tekstów o tej samej długości. Dodajemy je litera po literze, na przykład:

```
  MOJE_HASLO_DO_ SEJFU_TO_⇑QWER⇓
+BEZ_SERC_BEZ_DUCHA_TO_SZKIELE
 SBGSEYDJPESOMF→K⇓CAH↵MEROY/OV
```

Dodawanie bitów, a co za tym idzie – także dodawanie liter i tekstów, ma pewne pożyteczne własności. W szczególności jeżeli do jakiejś litery x dodamy

Dla każdych liter x, y i z zachodzą bowiem równości:

$$x + (y + z) = (x + y) + z,$$
$$x + y = y + x,$$
$$x + / = x,$$
$$x + x = /.$$

Z tego łatwo wynika, że:

$$(x + y) + y = x.$$

dwukrotnie inną literę y, to otrzymamy z powrotem x (patrz margines). Ta obserwacja stanowi podstawę szyfru Vernama. Aby skorzystać z tego szyfru, nadawca i odbiorca muszą zawczasu uzgodnić jakiś długi ciąg znaków K jako klucz szyfrujący. Następnie, aby zaszyfrować jakiś tekst T, nadawca dodaje go – litera po literze – do klucza szyfrującego. Powstały w ten sposób szyfrogram $S = T + K$ przesyła odbiorcy, który, odebrawszy go, dodaje doń ten sam klucz szyfrujący i odzyskuje $S + K = T$.

Przykładowo, jeżeli obie strony uzgodniły, że ich tajnym kluczem będzie tekst *Ody do młodości* Mickiewicza, to po odebraniu zaszyfrowanego komunikatu odbiorca wykona dodawanie i odzyska oryginalny tekst:

```
 SBGS EYDJ PESO M F →K⇓CA H↵M EROY/OV
+BEZ_ SERC_BEZ_ D U CHA_ TO_ SZKIELE
-----------------------------------
 MOJE _HASLO_DO_ S EJFU _TO _⇑QWER⇓
```

Zauważmy, że zaszyfrowanie i odszyfrowanie tekstu to dokładnie ta sama procedura. To jest duża zaleta szyfru Vernama, bo znacznie upraszcza konstruowanie maszyn szyfrujących tą metodą. Jedna maszyna dodająca ciągi znaków nadaje się zarówno do szyfrowania, jak i do odszyfrowywania komunikatów.

Wszystko to jest bardzo eleganckie, ale jak wybrać klucz szyfrujący, aby nasz szyfr był bezpieczny? To wcale nie jest łatwa sprawa. Początkujący szyfrant mógłby na przykład ustalić klucz składający się z jednej litery powtórzonej wiele razy:

```
 MO J E_HASLO_DO_SE J FU_TO_⇑QWER⇓
+DD D DDDDDDDDDDDDD DDDDDDDDDDDD
-------------------------------
 YZ→↵F XRN⇑ZF/ZFN↵→_CFBZFLVG↵AP
```

Otrzymujemy w ten sposób prosty szyfr podstawieniowy, w którym każda litera jest zastępowana przez inną zgodnie z raz na zawsze ustaloną zasadą. Wiadomo od stuleci, że takie szyfry można łatwo łamać, analizując częstość występowania liter w zaszyfrowanych tekstach. W tym przypadku jest jeszcze gorzej: takich „jednoliterowych” kluczy szyfrujących jest tylko 31, więc kryptoanalityk może łatwo wypróbować je wszystkie po kolei.

Może więc *Oda do młodości*, jak w poprzednim przykładzie? To jest trochę lepszy pomysł, ale tylko trochę. Jeżeli raz na zawsze ustalimy, że kluczem szyfrującym jest na przykład jakaś książka, to należy zakładać, że po pewnym czasie obcy szpiedzy dowiedzą się, jaka to książka, i od tej pory będą mogli swobodnie czytać wszystkie nasze komunikaty.

Jest też inny, poważniejszy problem. Nawet jeżeli ustalimy zupełnie nieznany naszym przeciwnikom klucz, ale kiedykolwiek użyjemy tego klucza więcej niż raz, to wystawiamy się na skuteczny atak. Taką sytuację nazywamy *głębią*.

Atak na głębię

Przypuśćmy, że dwa teksty T_1 i T_2 zaszyfrowaliśmy tym samym kluczem K, otrzymując dwa szyfrogramy:

$$T_1 + K = S_1, \qquad T_2 + K = S_2.$$

Jeżeli nasz przeciwnik zdołał podsłuchać oba szyfrogramy, to może dodać je do siebie litera po literze, otrzymując sumę oryginalnych tekstów:

$$S_1 + S_2 = (T_1 + K) + (T_2 + K) = \\ = (T_1 + T_2) + (K + K) = T_1 + T_2.$$

Zauważmy, że z tej sumy całkowicie zniknął klucz szyfrujący.

Co dalej mógłby z tym zrobić nasz przeciwnik – kryptoanalityk? Rozważmy to na przykładzie. Przypuśćmy, że przechwyciliśmy dwa szyfrogramy, które podejrzewamy, że były zaszyfrowane tym samym kluczem, i dodajmy je do siebie:

```
 MQFJO E WS⇑HB↵V F BQW⇑OL/R⇓TOPDKX
+GIEEY A L⇓NDOW↵ K NKAKQWBOTICFS↵M
---------------------------------
 IZNRF→EGQXE⇑P→YOTHKEBLKPP⇑NUE
```

Rozwiązanie zadania F 1072.
Gęstość ludzkiego ciała jest w przybliżeniu równa gęstości wody („leżąc” spokojnie w wodzie, nie toniemy), a więc nasza objętość równa się naszej masie podzielonej przez gęstość wody ρ_0. Siła wyporu powietrza powoduje zatem, że wskazywany przez wagę ciężar $Q = Q_0(1 - \rho/\rho_0)$. Gdyby nie było atmosfery, to na wysokości h nad Ziemią nasz ciężar wynosiłby:

$$Q = Q_0 \frac{R^2}{(R+h)^2} \approx Q_0 \left(1 - 2\frac{h}{R}\right).$$

Oznacza to, że bez atmosfery na wysokości

$$h \approx \frac{\rho R}{2\rho_0}$$

nasz ciężar byłby równy wskazaniom wagi na powierzchni Ziemi w obecności atmosfery. Po podstawieniu danych liczbowych otrzymujemy: $h \approx 4160$ m – wysokość bliska wysokości szczytu Jungfrau w Alpach Berneńskich.

Rozwiązanie zadania M 1746.
Skoro zbiór A zawiera 300 uczniów, to istnieje szkoła, w której uczy się co najwyżej 100 uczniów ze zbioru A. Niech będzie to szkoła S_1. Wtedy zbiór $A \setminus S_1$ ma co najmniej 200 uczniów. Zauważmy, że na mocy założeń każdy z uczniów z tego zbioru ma różną liczbę znajomych w S_1. Ponadto każdy z nich ma przynajmniej jednego znajomego w szkole S_1. Oznacza to, że każda liczba ze zbioru $\{1, 2, \ldots, 200\}$ musi być osiągana jako liczba znajomych ze szkoły S_1 kogoś ze zbioru $A \setminus S_1$. Wobec tego istnieje uczeń z $A \setminus S_1$, który zna wszystkich ze szkoły S_1. Bez straty ogólności załóżmy, że jest to uczeń x ze szkoły S_2. Wtedy na podstawie założeń zadania istnieje uczeń $y \in S_3$, że x i y się znają. Ponadto istnieje też uczeń z ze szkoły S_1, że y i z się znają. Jednakże x zna się z z, gdyż x zna wszystkich ze szkoły S_1. Zatem trójka uczniów (x, y, z) spełnia warunki zadania.

To nie wygląda sensownie, ale też suma dwóch sensownych tekstów w języku polskim nie ma powodu wyglądać sensownie. Żeby coś z tym zrobić, potrzebujemy jakiejś choćby szczątkowej informacji o tekstach, które chcemy odszyfrować. Może to być na przykład lista często występujących słów, których się spodziewamy w zaszyfrowanych komunikatach. Takie słowa nazywamy *ściągami*. Kryptolodzy w Bletchley Park szukali ściąg takich, jak *geheim* (niem. tajne), *nicht in Frage* (niem. wykluczone) czy *keine besonderen Ereignisse* (niem. bez szczególnych zdarzeń). Do znalezienia dobrych ściąg konieczna była znakomita znajomość języka, żargonu używanego w niemieckiej armii, a nawet ostatnich wydarzeń na froncie czy wręcz aktualnej prognozy pogody.

Przypuśćmy, że w jednym z zaszyfrowanych komunikatów może pojawić się słowo HASLO. Może nawet na samym początku? Jak musiałyby wyglądać pierwsze znaki drugiego komunikatu, aby suma tych komunikatów zaczynała się od znaków IZNRF? Pamiętając, że $X + Y = Z$ wtedy i tylko wtedy, gdy $X + Z = Y$, policzmy:

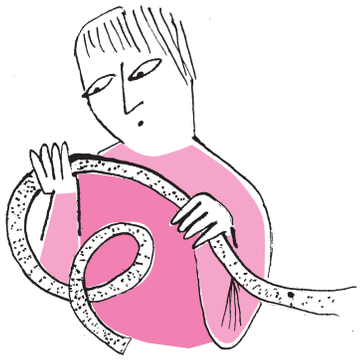
```
  IZNRF→EGQXE⇑P→YOTHKEBLKPP⇑NUE
+ HASLO
-------------------------------
  LLDOY
```

To nie wygląda na początek tekstu w języku polskim. A może na kolejnej pozycji?

```
  I ZNRF→EGQXE⇑P→YOTHKEBLKPP⇑NUE
+ _ HASL O
-------------------------------
  →SKK⇓T
```

To wygląda jeszcze gorzej. Próbując jednak kolejnych dopasowań, w końcu dojdziemy do:

```
  IZNRF→ EGQXE⇑ P →YOTHKEBLKPP⇑NUE
+          _HASLO_
-------------------------------
           SCHOWAL
```



Bingo! Nie dość, że zapewne trafiliśmy, to poznaliśmy też fragment drugiego komunikatu, a w dodatku możemy spróbować zgadnąć kilka jego kolejnych liter. Jest tu kilka możliwości: schował (i spacja), schowałem, schowaliśmy... Możemy wypróbować je po kolei i wkrótce zidentyfikujemy najbardziej obiecującą możliwość:

```
  IZNRF→ EGQXE⇑ P →YOTHKEBLKPP⇑NUE
+        _SCHOWAL EM_
-------------------------------
         I_HASLO_ ADM
```

Cierpliwy Czytelnik może spróbować ułożyć tę układankę do końca. Nie zawsze daje się w ten sposób odszyfrować cały komunikat (czasem słowa czy zdania kończą się w obu komunikatach w tym samym miejscu i trudno z tego miejsca ruszyć dalej), ale taki *atak na głębię* często pozwala poznać fragmenty obu komunikatów.

Widzimy więc, że dobry klucz szyfrujący powinien być niepowtarzalny, a przy tym pozbawiony jakiejś łatwej do zidentyfikowania struktury. Dlatego najlepiej za klucz przyjąć całkowicie losowy ciąg znaków. Jest to tak zwany szyfr klucza jednorazowego, który z punktu widzenia kryptografii jest doskonale bezpieczny: żadną metodą nie da się go złamać. Niestety, aby taki szyfr zastosować w praktyce, nadawca i odbiorca muszą zawczasu uzgodnić wspólny losowy ciąg znaków o długości co najmniej takiej, jak wszystkie komunikaty, które planują przesyłać. Szyfr klucza jednorazowego znalazł pewne ograniczone zastosowania, ale trudno sobie wyobrazić jego używanie do komunikacji na szeroką skalę.

Tak zwana gorąca linia między Pentagonem a Kremlem w latach sześćdziesiątych była oparta na szyfrze klucza jednorazowego i na kurierach, którzy pocztą dyplomatyczną przewozili długie ciągi losowych bitów.

Kompromisowym rozwiązaniem jest zastąpienie ciągu losowego pseudolosowym, generowanym przez maszynę. Jeżeli obie strony komunikacji używają takiej samej maszyny, to wystarczy, że uzgodnią początkowe ustawienia maszyny, a klucze wygenerowane po obu stronach będą identyczne. Głównym zadaniem maszyny Lorenz SZ40/42 było właśnie generowanie pseudolosowych ciągów znaków w alfabecie telegraficznym. Mimo skomplikowanej konstrukcji opartej na 12 kołach zębatych Anglikom udało się rozszyfrować jej działanie jedynie na podstawie przesyłanych komunikatów. O tym, jak tego dokonali, opowiemy w kolejnym numerze.