Algorytm Szyfru Atbasz

Szyfr Atbasz to prosty monoalfabetyczny szyfr podstawieniowy pochodzenia hebrajskiego, którego działanie polega na zamianie litery leżącej w odległości X od początku alfabetu na literę leżącą w odległości X od jego końca. Nazwa pochodzi od pierwszej, ostatniej, drugiej i przedostatniej litery alfabetu hebrajskiego: **A**lef→ **T**aw → **Be**t → **Sz**in.

Szyfr ten występuje w Biblii, w księdze Jeremiasza. Pojawia się w trzech wersetach.

1. Jeremiasza 25:26 – "*A król Szeszaku wypije po nich*" – Szeszak oznacza tu Babilon (בבל **bbl** → ששך **ššk**).
2. Jeremiasza 51:1 – "*Wzbudzam przeciw Babilonowi i mieszkańcom Leb-Kamaj niszczycielski wiatr*." – Leb-Kamaj oznacza Chaldejczyków (כשדים **kśdym** → לבקמי **lbqmy**).
3. Jeremiasza 51:41 – "*Jakże Szeszak został zdobyty, jakże Chwała całej ziemi została pojmana! Jakże Babilon stał się wśród narodów czymś, co budzi grozę!*" – Szeszak oznacza tu Babilon (בבל **bbl** → ששך **ššk**).

Księga Jeremiasza była spisywana w czasach niewoli babilońskiej. Jej egzemplarze były czytane przez Żydów przebywających w Babilonie. Korzystne więc byłoby, żeby w tekstach nieprzychylnych Babilonii nie pojawiały się wyraźne odniesienia przeciw jej królom.

◢→	Alef	Bet	Gimel	Dalet	He	Waw	Zajin	chet	Tet	Jod	Kof
Tekst jawny	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
◢←	Taw	Szin	Resz	Koof	Cade	Peh	Ajin	Samech	Nun	Mem	Lamed
Tekst zaszyfrowany	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל

◢→	Lamed	Mem	Nun	Samech	Ajin	Pe	Cade	Kuf	Resz	Szin	Taw
Tekst jawny	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
◢←	Kof	Jod	Tet	chet	Zajin	Waw	He	Dalet	Gimel	Bet	Alef
Tekst zaszyfrowany	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Przesuwając korelację w lewo lub w prawo, można wyprowadzić wariant **Batgasz** (nazwany na cześć Bet-Taw – Gimel –Szin) lub **Aszbar** (dla Alef-Szin-Bet-Reisz). Albo alternatywne odwzorowanie pozostawia jedną literę niepodstawioną; odpowiednio Alef i Taw.

Szyfr Atbasz dla alfabetu łacińskiego

Szyfr może być zastosowany również dla podstawowego alfabetu łacińskiego.

Tekst jawny	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
Tekst zaszyfrowany	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Wersja skrócona – prostsza do szyfrowania i deszyfrowania

Tekst jawny	A	B	C	D	E	F	G	H	I	J	K	L	M
Tekst zaszyfrowany	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

KRYPTOGRAFIA → PIBKGLTIZURZ

Zaletą tej metody jest prostota i łatwość tworzenia kolejnej odmiany szyfru.

Właściwości szyfru Atbasz

Jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego jest zastępowana inną. Szyb Atbasz może być postrzegany jako szczególny przypadek szyfru afinicznego.

Ponieważ istnieje tylko jeden sposób szyfrowania, algorytm Atbasz nie zapewnia bezpieczeństwa komunikacji, ponieważ nie ma żadnego klucza.

Możliwe jest użycie różnych sposobów podstawiania, ale nie zapewnia to większego bezpieczeństwa. Wystarczy tylko znajomość kilku liter, by znaleźć algorytm szyfrowania.

Kryptoanaliza:

Podstawową metodą jest ***analiza częstości***. Zestawienie częstości liter tekstu zaszyfrowanego należy porównać z częstością liter dla danego języka. Szyfr ten ma pewne charakterystyczne wartości, co pozwala na domyślenie się, że to właśnie atbasz.

Inną metodą jest próba odkrycia użytego hasła. Stosuje się tu ***metodę słów prawdopodobnych*** wynikającą ze znajomości poruszanej tematyki i osób posługujących się tym szyfrem. Odczytanie fragmentu wiadomości pozwala na złamanie reszty szyfru. Inną metodą jest ***metoda słownikowa*** stosowana, gdy wcześniejsza nie dała wyniku.

Można też użyć specjalnych tekstów:

- Wiadomością pozwalającą złamać szyfr jest ciąg kolejnych liter alfabetu (**abcdefghijklmnopqrstuvwxyz**). Dzięki temu możliwe jest ustalenie użytego szyfru.

Ćwiczenia

1. Używając szyfru Atbasz napisz program:
    a. szyfrujący wiadomość
    b. deszyfrujący wiadomość

    Program ma wczytywać tekst jawny i do szyfrowania.