ZŁAM TEN KOD Z PYTHONEM

JAK TWORZYĆ, TESTOWAĆ I ŁAMAĆ SZYFRY

AL SWEIGART

Helion

Tytuł oryginału: Cracking Codes with Python: An Introduction to Building and Breaking Ciphers

Tłumaczenie: Agnieszka Górczyńska

ISBN: 978-83-283-7495-9

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
https://ftp.helion.pl/przyklady/zlamtk.zip

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/zlamtk
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

1

Papier jako narzędzie kryptograficzne

„Dżin szyfrowania opuścił butelkę”.
— Jan Koum, założyciel WhatsApp

ZANIM PRZYSTĄPIMY DO TWORZENIA PROGRAMÓW SZYFRUJĄCYCH, WARTO ZAPOZNAĆ SIĘ Z PROCESEM SZYFROWANIA I DESZYFROWANIA WIADOMOŚCI Z UŻYCIEM PAPIERU I OŁÓWKA. TO POMOŻE ZROZUMIEĆ, JAK działa szyfrowanie i jakie operacje matematyczne są stosowane do wygenerowania zabezpieczonych wiadomości. Z tego rozdziału dowiesz się, co oznacza kryptografia i czym kod różni się od szyfru. Następnie użyjesz prostego szyfru zwanego szyfrem Cezara, aby zaszyfrować i odszyfrować wiadomość za pomocą papieru i ołówka.

TEMATY OMÓWIONE W TYM ROZDZIALE:

- co to jest kryptografia;
- kody i szyfry;
- szyfr Cezara;
- krążki szyfrowania;
- kryptografia i arytmetyka;
- podwójne szyfrowanie.

Co to jest kryptografia?

W przeszłości każdy, kto musiał udostępniać tajne informacje innym osobom, np. szpieg. żołnierz, haker, pirat, sprzedawca, tyran czy działacz polityczny, korzystał z kryptografii, aby informacje te nie wpadły w niepowołane ręce. *Kryptografia* to nauka stosowania tajnych kodów. Jeżeli chcesz się dowiedzieć, na czym polega idea kryptografii, spójrz na dwa przedstawione tutaj fragmenty kodu:

```
nyr N .vNwz5uNz5Ns662ONzON3z2v      !NN2 Nuwv,N9,vNN!vNrBN3zyN4vN
N yvNwz9vNz5N6!9Nyvr9               N6 QvvOz6nvN.7NOyv4N 4 zzvNN
yOQNnvNwv tyNz                      vyN,NN99zOzz6wzOy3vv26 9
Nw964N6!9N5vzxys69O,N.vN2z5u-       w296vyNNrrNyQst.56ON94Nu5y
3vNz Nr Ny64v,N .vNt644!5ztr vNz    rN5nz5vv5t6v63zNr5.
N 6N6 yv9O,Nr5uNz Nsvt64vON         N75sz6966NNvw6 zuO wtNxs6t
yvN7967v9 BN6wNr33Q N-m63 rz9v      49NrN3Ny9Nvzy!
```

Tekst w lewej kolumnie to tajna wiadomość, która została *zaszyfrowana*, czyli zmieniona na tajny kod. Pozostaje ona całkowicie nieczytelna dla każdego, kto nie wie, jak należy ją *deszyfrować*, czyli zmienić z powrotem na pierwotną postać. Tekst w prawej kolumnie to ciąg przypadkowo wybranych znaków, bez ukrytego znaczenia. Szyfrowanie pozwala na ukrycie wiadomości przed osobami, które nie potrafią jej odszyfrować, nawet jeśli w ich ręce wpadnie zaszyfrowana wiadomość. *Wiadomość zaszyfrowana wygląda dokładnie tak samo jak pozbawiony sensu ciąg znaków i cyfr.*

Kryptograf stosuje i analizuje tajne kody. Oczywiście te tajne wiadomości nie zawsze takimi pozostają. Z kolei *kryptoanalityk*, nazywany również *hakerem* (lub *łamaczem kodów*), może złamać kod i odczytać zaszyfrowane wiadomości. Z tej książki dowiesz się, jak szyfrować i deszyfrować wiadomości za pomocą różnych technik. Jednak wiedza ta nie jest na tyle niebezpieczna, aby zaprowadzić Cię za kratki.

Kod a szyfr

W przeciwieństwie do szyfru *kod* ma być doskonale zrozumiały i dostępny publicznie. Kod zastępuje wiadomość symbolami, które każdy powinien potrafić odczytać i zamienić na postać pierwotnej wiadomości.

Na początku XIX wieku powstał doskonale znany kod dzięki opracowaniu telegrafu, który umożliwił niemal natychmiastową komunikację przewodową między kontynentami. Wysłanie wiadomości za pomocą telegrafu było znacznie szybsze niż skorzystanie z którejś z dotychczasowych możliwości, np. posłańca na koniu lub listu napisanego na papierze. Telegraf pozwalał wysyłać jedynie dwa rodzaje impulsów elektrycznych: krótki, nazywany kropką, i długi, nazywany kreską.

Aby skonwertować litery alfabetu na owe kropki i kreski, potrzebny był system kodowania pozwalający zamienić słowa na impulsy elektryczne. Proces konwersji słów na kropki i kreski oraz ich przesyłania przez telegraf jest nazywany *kodowa-*

niem, proces odwrotny zaś nosi nazwę *dekodowania*. Kod używany podczas kodowania i dekodowania wiadomości przekazywanych poprzez telegraf (a później także radiowo) został opracowany przez Samuela Morse'a i Alfreda Vaila i nosi nazwę kodu Morse'a. Przedstawiłem go w tabeli 1.1.

Tabela 1.1. Międzynarodowy kod Morse'a

Litera	Kod	Litera	Kod	Liczba	Kod
A	• —	N	— •	1	• — — — —
B	— • • •	O	— — —	2	• • — — —
C	— • — •	P	• — — •	3	• • • — —
D	— • •	Q	— — • —	4	• • • • —
E	•	R	• — •	5	• • • • •
F	• • — •	S	• • •	6	— • • • •
G	— — •	T	—	7	— — • • •
H	• • • •	U	• • —	8	— — — • •
I	• •	V	• • • —	9	— — — — •
J	• — — —	W	• — —	0	— — — — —
K	— • —	X	— • • —		
L	• — • •	Y	— • — —		
M	— —	Z	— — • •		

Dzięki generowaniu kropek i kresek za pomocą jednoprzyciskowego telegrafu jego operator mógł przekazywać, niemalże natychmiast, wiadomości do osoby znajdującej się na drugim końcu świata. (Jeżeli chcesz dowiedzieć się więcej na temat kodu Morse'a, zajrzyj na stronę *https://pl.wikipedia.org/wiki/Kod_Morse'a*).

W przeciwieństwie do kodu szyfr to specjalny rodzaj kodu przeznaczony do zapewnienia tajności przekazywanym wiadomościom. Szyfr można wykorzystać do zmiany całkowicie jawnego tekstu, np. w języku angielskim, nazywanego *zwykłym tekstem*, w pozbawiony sensu ciąg liter i znaków, nazywany *szyfrogramem*, zawierający tajną wiadomość. Szyfr to zbiór reguł dotyczących konwersji między postaciami zwykłego tekstu i szyfrogramu. Te reguły często podczas komunikacji wykorzystują do szyfrowania i deszyfrowania tajny klucz, który jest znany tylko komunikującym się stronom. W niniejszej książce poznasz kilka szyfrów oraz utworzysz kilka stosujących je programów do szyfrowania i deszyfrowania wiadomości. Jednak najpierw zobacz, jak wiadomość można zaszyfrować ręcznie za pomocą papieru i ołówka.

Szyfr Cezara

Pierwszym szyfrem przedstawionym w tej książce będzie szyfr Cezara. Jego nazwa pochodzi od nazwiska Juliusza Cezara, który stosował go ponad 2000 lat temu. Dobra wiadomość jest taka, że szyfr ten jest prosty i dość łatwy do opanowania. Złą wiadomością jest to, że owa prostota oznacza możliwość łatwego złamania tego szyfru przez kryptoanalityka. Mimo to nadal jest użyteczny do zastosowania w celach edukacyjnych.

Szyfr Cezara działa poprzez zastąpienie każdej litery wiadomości inną literą, po przesunięciu całego alfabetu o określoną liczbę pozycji. Przykładowo Juliusz Cezar zastępował litery wiadomości przez przesunięcie liter alfabetu o trzy — każda litera wiadomości była zastępowana literą oddaloną od niej w alfabecie o trzy pozycje.

W omawianym przykładzie każde wystąpienie litery A w wiadomości będzie zastąpione literą D, każde wystąpienie litery B będzie zastąpione literą E itd. Gdy Cezar musiał przesunąć literę znajdującą się na końcu alfabetu, np. Y, wówczas przechodził na początek alfabetu i przesuwał ją o wymaganą liczbę pozycji, co oznacza, że np. literę Y zastąpi litera B. W tym podrozdziale ręcznie zaszyfrujesz wiadomość za pomocą szyfru Cezara.

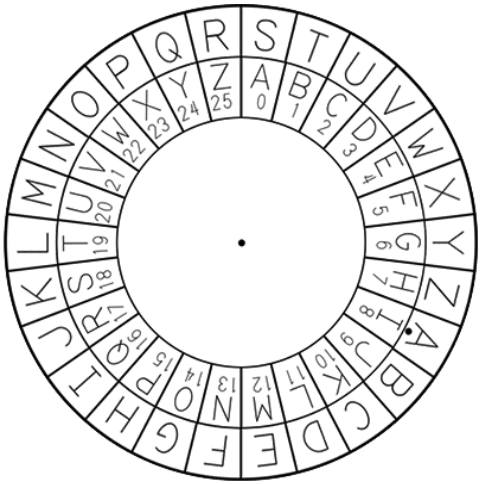
Krążek szyfrowania

Aby ułatwić sobie zadanie konwersji wiadomości w postaci zwykłego tekstu na szyfrogram z użyciem szyfru Cezara, można skorzystać z tzw. *krążka szyfrowania*, nazywanego również *dyskiem szyfrowania*. Krążek szyfrowania składa się z dwóch pierścieni liter, a każdy z nich jest podzielony na 26 slotów (po jednym dla każdej litery alfabetu). Pierścień zewnętrzny przedstawia alfabet zwykłego tekstu, natomiast pierścień wewnętrzny przedstawia litery szyfrogramu. W pierścieniu wewnętrznym litery są ponumerowane od 0 do 25. Te liczby stanowią tzw. *klucz szyfrowania*, który w omawianym przykładzie określa wielkość przesunięcia pierścienia zewnętrznego względem litery A w pierścieniu wewnętrznym. Ponieważ tarcza jest okrągła, przesunięcie o wartość klucza większą niż 25 powoduje powrót na początek alfabetu. Dlatego klucz 26 odpowiada przesunięciu o zero slotów, klucz 27 odpowiada przesunięciu o jeden slot itd.

Na stronie *https://inventwithpython.com/cipherwheel/* znajduje się internetowa wersja krążka szyfrowania. Pokazałem ją również na rysunku 1.1. Użycie internetowego krążka szyfrowania wymaga jego kliknięcia myszą i przesunięcia kursora aż do otrzymania żądanej konfiguracji. Następnie należy ponownie kliknąć myszą i tym samym zakończyć możliwość obracania pierścienia zewnętrznego.

W witrynie internetowej poświęconej tej książce znajdziesz krążek szyfrowania w wersji przeznaczonej do wydruku. Wytnij oba koła i ułóż je, mniejsze na środku większego. Następnie w środku wbij szpilkę, aby móc obracać koła.

W ten sposób będziesz mógł szyfrować wiadomości za pomocą krążka szyfrowania.



S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Rysunek 1.1 Internetowa wersja krążka szyfrowania

Szyfrowanie wiadomości za pomocą krążka szyfrowania

Jeżeli chcesz zaszyfrować wiadomość, najpierw musisz ją zapisać na kartce. W omawianym przykładzie zaszyfrujemy następującą wiadomość: `THE SECRET PASSWORD IS ROSEBUD`. Następnie obracaj pierścień wewnętrzny, aż dopasujesz sloty z pierścieniem zewnętrznym. Zwróć uwagę na kropkę znajdują się pod literą A w pierścieniu zewnętrznym. Zanotuj liczbę w slocie pierścienia wewnętrznego odpowiadającym tej literze A. To jest nasz klucz szyfrowania.

Przykładowo na rysunku 1.1 litera A w pierścieniu zewnętrznym znajduje się nad liczbą 8 w pierścieniu wewnętrznym. Wykorzystamy ten klucz szyfrowania, aby przygotować zaszyfrowaną wersję naszej wiadomości (zobacz rysunek 1.2).

T	H	E		S	E	C	R	E	T		P	A	S	S	W	O	R	D		I	S		R	O	S	E	B	U	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	P	M		A	M	K	Z	M	B		X	I	A	A	E	W	Z	L		Q	A		Z	W	A	M	J	C	L

Rysunek 1.2. Szyfrowanie wiadomości za pomocą szyfru Cezara i klucza szyfrowania o wartości 8

Każdą literę wiadomości odszukaj w pierścieniu zewnętrznym i zastąp odpowiadającą jej literą z pierścienia wewnętrznego. W omawianym przykładzie pierwsza litera wiadomości to *T* (w słowie *THE*). Po odszukaniu litery T w pierścieniu zewnętrznym zobaczysz, że odpowiadającą jej literą pierścienia wewnętrznego jest *B*. Dlatego w tajnej wiadomości litera T zawsze będzie zastępowana literą B. (Jeżeli używasz innego klucza szyfrowania, każde wystąpienie litery T zostanie zastąpione

inną literą). Następna litera w naszej wiadomości to H, która ma być zastąpiona literą P. Kolejna litera to E, którą należy zastąpić literą M. Każda litera pierścienia zewnętrznego zawsze powoduje zaszyfrowanie tej samej litery pierścienia wewnętrznego. Aby zaoszczędzić nieco czasu, po wyszukaniu pierwszej litery T i sprawdzeniu, że po zaszyfrowaniu to litera B, można od razu zastąpić wszystkie wystąpienia litery T w wiadomości literą B i dzięki temu tylko jednokrotnie sprawdzać daną literę.

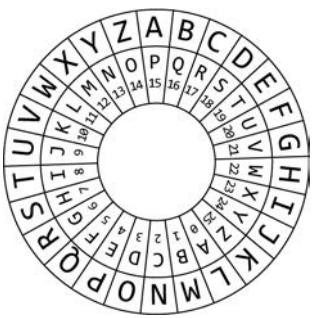
Po zaszyfrowaniu pierwotna wiadomość `THE SECRET PASSWORD IS ROSEBUD` będzie miała postać `BPM AMKZMB XIAAEWZL QA ZWAMJCL`. Zwróć uwagę na to, że znaki inne niż litery, np. spacja, pozostają bez zmian.

Teraz tę wiadomość można wysłać do kogoś (lub zachować ją dla siebie), a nikt nie będzie w stanie jej odczytać, dopóki nie otrzyma klucza szyfrowania. Nie ujawniaj nikomu klucza szyfrowania. Szyfrogram będzie mógł zostać odczytany przez każdego, kto wie, że kluczem szyfrowania jest 8.

Deszyfrowanie za pomocą krążka szyfrowania

Aby deszyfrować szyfrogram, trzeba rozpocząć od pierścienia wewnętrznego i następnie przejść do pierścienia zewnętrznego. Załóżmy, że otrzymaliśmy taki oto szyfrogram: `IWT CTL EPHHLDGS XH HLDGSUXHW`. Nie będziesz w stanie odszyfrować tej wiadomości, jeśli nie znasz klucza (lub nie jesteś sprytnym hakerem). Na szczęście kolega poinformował Cię, że użył klucza szyfrowania 15. Krążek szyfrowania dla tego klucza pokazałem na rysunku 1.3.

Teraz możesz wyrównać literę A w pierścieniu zewnętrznym (tę z kropką na dole) z literą w pierścieniu wewnętrznym, która ma liczbę 15 (jest to P). Odszukaj pierwszą literę szyfrogramu, I, w pierścieniu wewnętrznym i zobacz, jaka odpowiada jej litera w pierścieniu zewnętrznym (jest to T). Druga litera szyfrogramu, W, po deszyfrowaniu to H. Procedurę deszyfrowania kontynuuj dla wszystkich liter szyfrogramu, a otrzymasz wiadomość `THE NEW PAS` ↪`SWORD IS SWORDFISH` w postaci zwykłego tekstu (zobacz rysunek 1.4).



Rysunek 1.3.Krążek szyfrowania z ustawionym kluczem 15

Jeżeli do deszyfrowania zostanie użyty niepoprawny klucz, np. 16, wówczas wiadomość będzie miała postać `SGD MDV OZRRVNQC HR RVNQCEHRG`, która

I	W	T		C	T	L		E	P	H	H	L	D	G	S		X	H		H	L	D	G	S	U	X	H	W
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
T	H	E		N	E	W		P	A	S	S	W	O	R	D		I	S		S	W	O	R	D	F	I	S	H

Rysunek 1.4. Deszyfrowanie wiadomości za pomocą szyfru Cezara i klucza szyfrowania o wartości 15

jest bez sensu. Dopóki nie zostanie zastosowany prawidłowy klucz, deszyfrowana wiadomość jest ciągiem przypadkowych liter.

Szyfrowanie i deszyfrowanie z użyciem arytmetyki

Krążek szyfrowania to wygodne narzędzie przeznaczone do szyfrowania i deszyfrowania wiadomości za pomocą szyfru Cezara. Jednak operacje szyfrowania i deszyfrowania można przeprowadzać również z wykorzystaniem arytmetyki. W tym celu litery alfabetu od A do Z trzeba zapisać za pomocą liczb od 0 do 25. W takim przypadku 0 odpowiada literze A, 1 odpowiada literze B itd., aż do liczby 25, która odpowiada literze Z. Te przypisania pokazałem na rysunku 1.5.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Rysunek 1.5. Numerowanie od 0 do 25 liter alfabetu

Ten kod „litera na liczbę” można wykorzystać do przedstawienia liter. Jest to potężna koncepcja, ponieważ pozwala przeprowadzać operacje matematyczne na literach. Przykładowo jeśli litery CAT odpowiadają liczbom 2, 0 i 19, można do tych liczb dodać 3 i tym samym otrzymać 5, 3 i 22. Te nowe liczby odpowiadają literom FDW, jak pokazałem na rysunku 1.5. „Dodaliśmy” jedynie 3 do słowa *cat*. W dalszej części książki utworzymy program, aby to komputer za nas wykonywał odpowiednie operacje matematyczne.

Jeżeli chcesz skorzystać z arytmetyki do szyfrowania za pomocą szyfru Cezara, odszukaj liczbę odpowiadającą literze przeznaczonej do szyfrowania, a następnie dodaj do niej wartość klucza. W efekcie otrzymasz sumę reprezentującą zaszyfrowaną literę. Przykładowo szyfrujemy wiadomość `HELLO. HOW ARE YOU?` z użyciem klucza 13. (Jako klucza można użyć dowolnej liczby z przedziału od 1 do 25). Zaczynamy od odszukania litery H, która odpowiada liczbie 7. Po dodaniu do niej klucza, 13, otrzymujemy wartość 20. Skoro liczbie 20 odpowiada litera U, zaszyfrowane H to U.

Podobnie szyfrujemy literę E (4), dodajemy wartość klucza i otrzymujemy liczbę 17, której odpowiada litera R. Zaszyfrowane E to zatem litera R. Dalej postępujemy według tej samej procedury.

Proces działa świetnie aż do litery O, której odpowiada liczba 14. Po dodaniu klucza, 13, otrzymujemy liczbę 27, a lista kończy się na wartości 25. Jeżeli suma litery i klucza jest większa lub równa 26, wówczas trzeba od niej odjąć 26. W omawianym przykładzie mamy 27 – 26 = 1. Literą odpowiadającą liczbie 1 jest B, więc litera O po zaszyfrowaniu będzie literą B. Po zaszyfrowaniu całej wiadomości otrzymamy szyfrogram: `URYYB. UBJ NER LBH?`.

Aby deszyfrować szyfrogram, wartość klucza trzeba odejmować, a nie dodawać. Literze B odpowiada liczba 1. Po odjęciu klucza, 13, otrzymujemy -12. Podobnie jak w przypadku reguły „odejmij 26” stosowanej przy szyfrowaniu, gdy podczas deszyfrowania wynik jest mniejszy niż 0, trzeba do niego dodać 26. Skoro –12 + 26 = 14, to literze B szyfrogramu odpowiada litera O.

UWAGA *Jeśli nie wiesz, jak dodawać i odejmować liczby ujemne, więcej informacji na ten temat znajdziesz na stronie* https://inventwithpython.com/chapter12.html#_Toc405145134.

Jak widać, do odszyfrowania wiadomości zabezpieczonej szyfrem Cezara nie musisz korzystać z krążka szyfrowania. Potrzebujesz jedynie papieru, ołówka i nieco prostej arytmetyki.

Dlaczego podwójne szyfrowanie nie działa?

Być może sądzisz, że dwukrotne zaszyfrowanie wiadomości z użyciem dwóch różnych kluczy może podwoić siłę szyfrowania. Jednak to nieprawda w przypadku szyfru Cezara (a także wielu innych szyfrów). Ponadto wynik podwójnego szyfrowania jest taki sam jak w przypadku zwykłego pojedynczego szyfrowania. Spróbujmy dwukrotnie zaszyfrować wiadomość, aby się przekonać, dlaczego tak się dzieje.

Przykładowo jeśli zaszyfrujemy słowo `KITTEN` z użyciem klucza 3, będziemy dodawać 3 do liczby reprezentującej literę wiadomości w postaci zwykłego tekstu i otrzymamy szyfrogram `NLWWHQ`. Gdy teraz ten ciąg tekstowy zaszyfrujemy ponownie, ale z użyciem klucza 4, otrzymamy szyfrogram `RPAALU`, ponieważ dodajemy 4 do liczby reprezentującej literę wiadomości w postaci zwykłego tekstu. Jednak ma to taki sam efekt jak jednokrotne zaszyfrowanie słowa `KITTEN` kluczem 7.

W przypadku większości szyfrów wielokrotne szyfrowanie nie przekłada się na jego większą siłę. A jeśli zaszyfrujesz tekst za pomocą dwóch kluczy o sumie wynoszącej 26, wynikowy szyfrogram będzie miał dokładnie taką samą postać jak wiadomość w postaci zwykłego tekstu!

Podsumowanie

Szyfr Cezara i inne szyfry były na przestrzeni wieków stosowane do szyfrowania tajnych wiadomości. Gdyby ktoś chciał zaszyfrować długi komunikat, np. całą książkę, taka operacja przeprowadzana ręcznie mogła zająć wiele dni lub tygodni. Tutaj z pomocą może przyjść programowanie. Komputer umożliwia szyfrowanie i deszyfrowanie ogromnych ilości tekstu w czasie poniżej sekundy!

Aby wykorzystać komputer do szyfrowania, należy go *zaprogramować*, czyli nakazać mu wykonanie dokładnie tych samych kroków, ale w postaci zrozumiałej dla maszyny. Na szczęście poznanie języka programowania takiego jak Python jest znacznie łatwiejsze niż nauczenie się języka obcego, np. japońskiego lub hiszpańskiego. Ponadto nie trzeba mieć zbyt dużej wiedzy z zakresu matematyki — wystarczy umiejętność dodawania, odejmowania i mnożenia. Musisz mieć do dyspozycji komputer i tę książkę!

Przechodzimy teraz do rozdziału 2., z którego dowiesz się, jak używać powłoki interaktywnej Pythona w celu wykonywania pojedynczych wierszy kodu.

ĆWICZENIA PRAKTYCZNE

Odpowiedzi do ćwiczeń zostały zamieszczone w dodatku B.

1. Zaszyfruj wyrażenia za pomocą podanego klucza.
   a) `Able to pick with equal skill a right-hand pocket or a left`, klucz 4: `AMBIDEXTROUS`
   b) `A machine which makes a Frenchman shrug his shoulders with good reason`, klucz 17: `GUILLOTINE`
   c) `Your irreverence toward my deity`, klucz 21: `IMPIETY`
2. Deszyfruj szyfrogramy za pomocą podanego klucza.
   a) `P RDHIJBT HDBTIXBTH LDGC QN HRDIRWBTC XC PBTGXRP PCS PBTGXRPCH XC HRDIAPCS`, klucz 15: `ZXAI`
   b) `E VMZEP EWTMVERX XS TYFPMG LSRSVW`, klucz 4: `MQTSWXSV`
3. Zaszyfruj zdanie `This is a silly example` z użyciem klucza 0.
4. Oto kilka słów i ich szyfrogramów. Jaki klucz został użyty do zaszyfrowania poszczególnych słów?
   a) `ROSEBUD` – `LIMYVOX`
   b) `YAMAMOTO` – `PRDRDFKF`
   c) `ASTRONOMY` – `HZAYVUVTF`
5. Jakie zdanie zostało zaszyfrowane kluczem 8 i deszyfrowane kluczem 9?
   `UMMSVMAA: Cvkwuuwv xibqmvkm qv xtivvqvo i zmdmvom bpib qa ewzbp epqtm`


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

A TERAZ STWÓRZ ALGORYTM SZYFRU IDEALNEGO!

Szyfrowanie do niedawna było wiązane z bezpieczeństwem publicznym. Najbezpieczniejsze implementacje podlegały takim samym rządowym regulacjom jak przemysł zbrojeniowy. Do dzisiaj rządy i różnego rodzaju służby dążą do uzyskania możliwości odczytywania zaszyfrowanych danych. Tymczasem silna kryptografia jest podstawą globalnej ekonomii, zapewnia codzienną ochronę milionom użytkowników i większości organizacji. A to nie wszystko. Algorytmy szyfrujące, ich implementacja czy programowe łamanie szyfrów to równocześnie fascynująca dziedzina wiedzy i pole do zabawy, ćwiczeń oraz eksperymentowania z programowaniem.

Ta książka jest przeznaczona dla osób, które nie umieją programować, ale chciałyby zapoznać się z kryptografią. Omówiono tu podstawowe koncepcje programowania w Pythonie, który dziś jest uważany za najlepszy język dla początkujących koderów. Pokazano, jak tworzyć, testować i łamać programy implementujące szyfry klasyczne, takie jak przestawieniowy i Vigenère'a, by stopniowo przejść do znacznie bardziej zaawansowanych zagadnień, w tym kryptografii klucza publicznego. Każdy program przedstawiono w postaci pełnego kodu źródłowego, wyjaśniono także wiersz po wierszu jego działanie. Dzięki tej książce można się zarówno nauczyć zasad kryptografii, jak i zdobyć umiejętności pisania kodu szyfrującego i deszyfrującego w Pythonie.

Znajdziesz tutaj między innymi:

- wprowadzenie do programowania w Pythonie: pętle, zmienne, kontrola przepływu działania programu
- omówienie technik szyfrowania stosowanych przed wynalezieniem komputerów
- różne algorytmy szyfrowania z wykorzystaniem Pythona
- testowanie programów szyfrujących i deszyfrujących
- szyfrowanie i deszyfrowanie plików
- łamanie szyfrów techniką *brute force* czy analiza częstotliwości

Al Sweigart jest zawodowym programistą, projektantem UI i autorem cenionych książek technicznych. Jego ulubionym językiem programowania jest Python. Uważany za utalentowanego nauczyciela kodowania, twórca wielu samouczków w tej dziedzinie. Obecnie mieszka w San Francisco.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-7495-9
9 788328 374959
Cena: 89,00 zł
no starch press