2. Szyfrujemy wiadomości

Szyfrów używano od wielu stuleci do utajniania korespondencji dworskiej oraz w wojsku do przesyłania pomiędzy oddziałami wiadomości, które nie powinny być czytane przez wroga. W XIX w., kiedy zaczęła się rozwijać kolej żelazna i upowszechniały się sposoby komunikacji na odległość (telegraf i teleks), metodami szyfrowania zainteresowali się również ludzie biznesu. W II połowie XX w., wraz z rozwojem telekomunikacji i globalnych sieci komputerowych, praktyka szyfrowania informacji stawała się coraz bardziej powszechna. Dziś dotyczy każdego z nas, gdyż stanowi podstawę bezpieczeństwa m.in. transakcji bankowych i płatności elektronicznych.

Cele lekcji

- Zrozumiesz podstawowe pojęcia związane z kryptografią.
- Dowiesz się, po co szyfruje się informacje i jakie są zastosowania kryptografii.
- Poznasz przykłady szyfrów podstawieniowych i przestawieniowych, w tym szyfr Cezara i szyfr kolumnowy.
- Napiszesz programy szyfrujące informacje tekstowe poznanymi metodami.
- Poznasz techniki łamania prostych szyfrów.

2.1. Podstawowe pojęcia kryptografii

Szyfrowanie

Szyfrowaniem nazywamy przekształcanie informacji do postaci trudnej do odczytania bez dodatkowej wiedzy. Celem szyfrowania jest zapewnienie tajności (poufności) informacji. Zagadnieniami związanymi z szyfrowaniem zajmuje się nauka zwana **kryptografią**.

Kryptografia

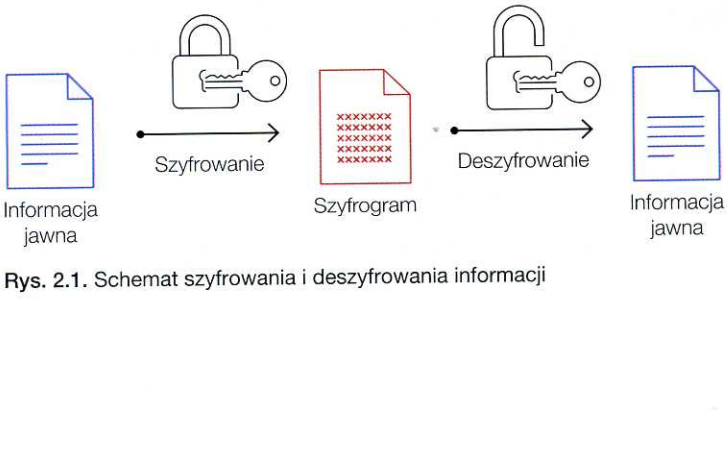
Tekst jawny

Szyfrogram

W trakcie szyfrowania informację jawną, zwaną **tekstem jawnym** (ang. *plaintext*), przekształca się w **szyfrogram** (ang. *ciphertext*), czyli tekst zaszyfrowany (rys. 2.1). W tym procesie stosuje się odpowiedni algorytm oraz **klucz szyfrowania** (ang. *cipher key*). Jest to pewna tajna wartość, niezależna od szyfrowanej informacji, która umożliwia **deszyfrowanie** zaszyfrowanej wiadomości. Warunkiem tajności informacji jest utrzymanie w tajemnicy klucza szyfrowania.

Klucz szyfrowania

Deszyfrowanie



Rys. 2.1. Schemat szyfrowania i deszyfrowania informacji

2.2. Szyfry przestaw

Pionierami w rozwoju kl
nie Spartanie. Grecki poe
o przyrządzie do szyfrowar
gruby kij), używanym w Sp

Zasada korzystania ze sk
nawijał na pałkę pasek pe
jących się fragmentach. Po
nieczytelna. Adresat posiad
tanie wiadomości. W tej r
i kształt wałka.

Poniżej zilustrowano spo
o kształcie graniastosłupa p

Odczytywanie wia na skytale

Po otrzymaniu szyfrogramu przek
go na wałek o ustalonej wcześniej

Szyfrogram:
TETSKAEKOTSWNSJTTNTTEEJ

Załóżmy, że niepowołana
domość oraz znała tę meto
wymiarów wałka, trudno j
musiałaby sprawdzić wiele w

Ćwiczenie 1

Przygotuj model urządzen
kiego paska papieru o dług
ny model skytale do zaszy

iadomości

korespondencji dworskiej
łami wiadomości, które nie
iedy zaczęła się rozwijać
munikacji na odległość
resowali się również ludzie
telekomunikacji i globalnych
formacji stawała się coraz
nas, gdyż stanowi podstawę
płatności elektronicznych.

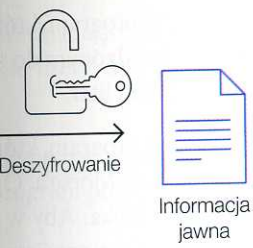
z kryptografią.
akie są zastosowania

ch i przestawieniowych, w tym

ekstowe poznanymi metodami.

grafii

anie informacji do postaci
edzy. Celem szyfrowania jest
cji. Zagadnieniami związany-
ana **kryptografią**.
rną, zwaną **tekstem jawnym**
gram (ang. *ciphertext*), czyli
ocesie stosuje się odpowied-
ng. *cipher key*). Jest to pewna
informacji, która umożliwia
ci. Warunkiem tajności infor-
a szyfrowania.



nformacji

2.2. Szyfry przestawieniowe. Szyfr kolumnowy

Pionierami w rozwoju klasycznej kryptografii byli prawdopodobnie Spartanie. Grecki poeta Archiloch w jednym z dzieł wspomniał o przyrządzie do szyfrowania zwanym **skytale** (od gr. *skútalon* – długi, gruby kij), używanym w Sparcie od VII w. p.n.e.

Skytale

Zasada korzystania ze skytale była następująca: nadawca wiadomości nawijał na pałkę pasek pergaminu (lub skóry) i pisał tekst na stykających się fragmentach. Po rozwinięciu paska wiadomość stawała się nieczytelna. Adresat posiadał identyczną pałkę, umożliwiającą odczytanie wiadomości. W tej metodzie szyfrowania **kluczem** są grubość i kształt wałka.

Klucz szyfrowania, s. 30

Poniżej zilustrowano sposób odczytywania szyfrogramu na skytale o kształcie graniastosłupa prawidłowego sześciokątnego.

Odczytywanie wiadomości zaszyfrowanej na skytale

Po otrzymaniu szyfrogramu przekazanego na pasku pergaminu należy nawinąć go na wałek o ustalonej wcześniej grubości. Grubość wałka jest kluczem tego szyfru.

Szyfrogram:
TETSKAEKOTSWNSJTTNTTEEJY

Tekst jawny:
TENTEKSTTOJESTTEKSTJAWNY

Załóżmy, że niepowołana osoba przechwyciła zaszyfrowaną wiadomość oraz znała tę metodę szyfrowania. Jeśli nie zna dokładnych wymiarów wałka, trudno jej będzie odczytać informację, ponieważ musiałaby sprawdzić wiele wałków o różnych grubościach.

Ćwiczenie 1

Przygotuj model urządzenia skytale i pergaminu: użyj ołówka i wąskiego paska papieru o długości ok. 25–30 cm. Wykorzystaj zbudowany model skytale do zaszyfrowania krótkiej wiadomości tekstowej.

Dobra rada

Wiele ołówków ma kształt graniastosłupa prawidłowego sześciokątnego. Możesz więc wykorzystać ołówek jako skytale.

Warto wiedzieć

Auguste Kerckhoffs oraz Claude Shannon niezależnie od siebie sformułowali tezę zwaną dziś zasadą Kerckhoffsa. Mówi ona, że zapewnienie poufności informacji nie powinno zależeć od utrzymania metody szyfrowania w tajemnicy – tajny powinien być wyłącznie klucz. Dzięki upublicznieniu szczegółów algorytmów szyfrujących można wykryć luki bezpieczeństwa, zanim algorytm zostanie wdrożony.

Szyfr przestawieniowy

Technikę szyfrowania, z której korzysta się w metodzie z użyciem skytale, nazywa się współcześnie **szyfrem przestawieniowym**. Szyfr ten polega na przestawieniu znaków z informacji jawnej. Szyfrogram i informacja jawna składają się więc z tych samych znaków, ale ustawionych w innej kolejności.

Szyfr kolumnowy

Szyfr kolumnowy

Innym szyfrem przestawieniowym, podobnym do metody z użyciem skytale, jest **szyfr kolumnowy**. Polega on na zapisaniu tekstu jawnego w wierszach, przy czym każdy wiersz (czasem z wyjątkiem ostatniego) składa się z takiej samej liczby znaków odpowiadającej liczbie kolumn. Kluczem szyfrowania jest liczba kolumn. Jeśli ostatni wiersz jest niepełny, można go uzupełnić dowolnymi znakami.

Dla tekstu jawnego PRZYNIESPRZESYLKEDOPARKU i klucza 4 zapis w kolumnach wygląda tak jak na rysunku 2.2.

P	R	Z	Y
N	I	E	S
P	R	Z	E
S	Y	L	K
E	D	O	P
A	R	K	U

Rys. 2.2. Podział tekstu jawnego na kolumny zgodnie z kluczem szyfrowania

Jeśli odczytamy znaki tekstu kolumnami (z góry na dół), otrzymamy tekst zaszyfrowany: PNPSEARIRYDRZEZLOKYSEKPU.

Warto wiedzieć

Informację zaszyfrowaną nazywa się czasami niepoprawnie informacją zakodowaną. Słowa „szyfr" i „kod" nie są synonimami. Kodu używamy, gdy nie można bezpośrednio przekazać informacji, np. ze względu na odległość. Przykładem kodu jest zapis za pomocą liter na papierze albo binarnie w komputerze. Szyfr to przekształcenie zapisu jawnego w niejawny, np. przez przestawienie kolejności liter lub bitów.

Ćwiczenie 2

Zaszyfruj tekst PRZYNIESPRZESYLKEDOPARKU, używając klucza o wartości 6.

A to ciekawe

Anagram jako szyfrogram

Niektórzy uczeni nie chcieli ogłaszać wprost treści swoich odkryć, dlatego stosowali anagramy, czyli zmieniali kolejność liter w zdaniu. Istotę odkrycia, zazwyczaj w formie łacińskiego anagramu, ogłaszali drukiem. W 1610 r. Galileusz opublikował w ten sposób swoje odkrycie dotyczące rzekomych księżyców Saturna: SMAISMRMILMEPOETALEVMIBVNENVGTTAVIRAS. Oznacza to: ALTISSIMUM PLANETAM TERGEMINUM OBSERVARI (dosł. widziałem najwyższą z planet potrójną). Liter U i V wtedy nie rozróżniano.