## Rozdział 2

# Klasyczna kryptografia

W tym rozdziale przedstawiamy ogólne wprowadzenie do kryptografii i kryptoanalizy. Prezentujemy kilka prostych systemów i opisujemy, jak można je „złamać". Po drodze omawiamy różne techniki matematyczne, które będą stosowane w całej książce.

## 2.1. Wprowadzenie: niektóre proste kryptosystemy

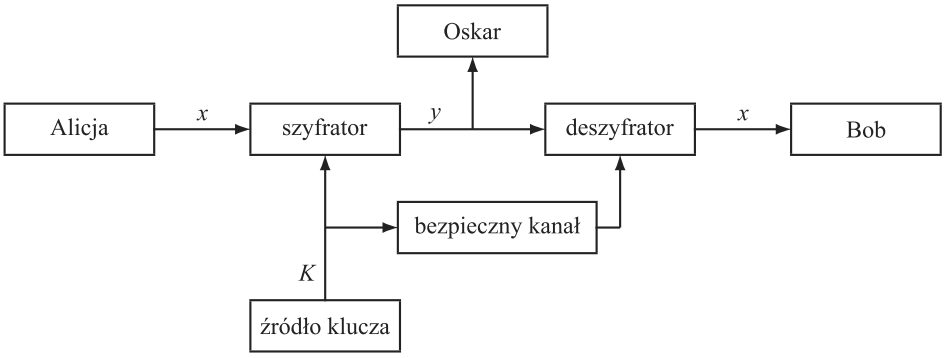
Podstawowym celem kryptografii jest umożliwienie dwóm osobom, zwanym zazwyczaj *Alicją* i *Bobem*, komunikowania się przez niepewny kanał w taki sposób, aby przeciwnik, *Oskar*, nie mógł zrozumieć, o czym jest mowa. Kanałem tym może być na przykład linia telefoniczna lub sieć komputerowa. Informacja, którą Alicja chce wysłać do Boba, nazywana „tekstem jawnym", może być angielskim (lub polskim) tekstem, danymi liczbowymi lub czymś innym – jej struktura jest całkowicie dowolna. Alicja szyfruje tekst jawny, używając uprzednio ustalonego klucza, i wysyła otrzymany w ten sposób szyfrogram przez kanał. Oscar, widząc dzięki podsłuchowi zaszyfrowany tekst w kanale, nie może określić, czym był tekst jawny, ale Bob, który zna klucz szyfrujący, może ten tekst odszyfrować i odtworzyć.

Pomysły te są formalnie opisane za pomocą następującego zapisu matematycznego.

**DEFINICJA 2.1.** Kryptosystem jest krotką pięcioelementową $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, która spełnia następujące warunki:

1. $\mathcal{P}$ jest skończonym zbiorem możliwych *tekstów jawnych*.
2. $\mathcal{C}$ jest skończonym zbiorem możliwych *szyfrogramów*.
3. $\mathcal{K}$, *przestrzeń kluczy*, jest skończonym zbiorem możliwych *kluczy*.
4. Dla każdego $K \in \mathcal{K}$ istnieje *reguła szyfrowania* $e_K \in \mathcal{E}$ i odpowiadająca jej *reguła odszyfrowania* $d_K \in \mathcal{D}$. Każda $e_K: \mathcal{P} \to \mathcal{C}$ i $d_K: \mathcal{C} \to \mathcal{P}$ są funkcjami takimi, że $d_K(e_K(x)) = x$ dla każdego elementu tekstu jawnego $x \in \mathcal{P}$.

Najważniejszą właściwością jest właściwość 4. Mówi ona, że jeśli test jawny $x$ został zaszyfrowany przy użyciu $e_K$, a otrzymany szyfrogram zostanie następnie odszyfrowany przy użyciu $d_K$, wynikiem będzie oryginalny tekst jawny $x$.




**RYSUNEK 2.1.** Kanał komunikacyjny

Alicja i Bob użyją następującego protokołu, aby wykorzystać konkretny kryptosystem. Najpierw wybierają losowy klucz $K \in \mathcal{K}$. Jest to wykonywane, gdy znajdują się w tym samym miejscu i nie są obserwowani przez Oskara, lub, alternatywnie, gdy mają dostęp do bezpiecznego kanału, w którym to przypadku mogą znajdować się w różnych miejscach. Przypuśćmy, że później Alicja chce przekazać wiadomość do Boba przez niepewny kanał. Przyjmujemy, że ta wiadomość jest *ciągiem znaków*

$$\boldsymbol{x} = x_1 x_2 \cdots x_n$$

dla pewnej liczby całkowitej $n \geqslant 1$, gdzie każdy symbol tekstu jawnego $x_i \in \mathcal{P}$, $1 \leqslant i \leqslant n$. Każdy $x_i$ został zaszyfrowany przy użyciu zasady szyfrowania $e_K$ określonej przez z góry ustalony klucz $K$. W ten sposób Alicja oblicza $y_i = e_K(x_i)$, $1 \leqslant i \leqslant n$, a otrzymany ciąg szyfrogramu

$$\boldsymbol{y} = y_1 y_2 \cdots y_n$$

jest przesyłany przez kanał. Gdy Bob otrzymuje $y_1 y_2 \cdots y_n$, odszyfrowuje go przy użyciu funkcji odszyfrowania $d_K$, uzyskując oryginalny ciąg tekstu jawnego, $x_1 x_2 \cdots x_n$; patrz rysunek 2.1 ilustrujący kanał komunikacyjny.

Oczywiście musi być spełniony warunek, że każda funkcja szyfrująca $e_K$ jest *funkcją różnowartościową* (tzn. jeden do jednego).W przeciwnym razie nie można by było przeprowadzić odszyfrowania w sposób jednoznaczny. Na przykład, jeżeli

$$y = e_K(x_1) = e_K(x_2), \tag{2.1}$$

gdzie $x_1 \neq x_2$, to Bob nie może wiedzieć, czy $y$ trzeba rozszyfrować jako $x_1$, czy jako $x_2$. Zwróćmy uwagę, że jeśli $\mathcal{P} = \mathcal{C}$, wynika z tego, że każda funkcja szyfrująca jest permutacją. Oznacza to, że jeśli zbiór tekstów jawnych i szyfrogramów jest identyczny, to każda funkcja szyfrująca po prostu przestawia (lub permutuje) elementy tego zbioru.