1. Wstęp

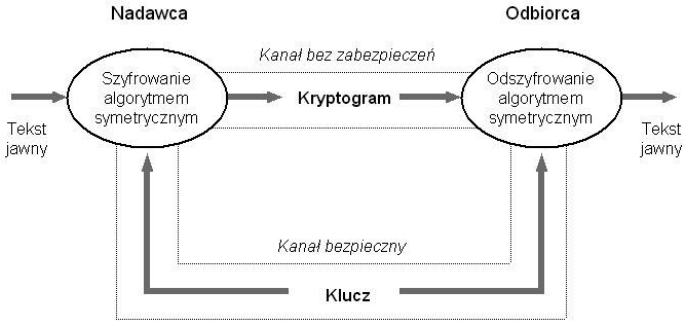
W systemach komputerowych zasadniczym problemem jest bezpieczne przesyłanie i przechowywanie informacji. W niniejszym opracowaniu przedstawiono problemy bezpiecznego przekazywania informacji w oparciu o jej szyfrowanie i deszyfrowanie. Zagadnieniami kryptografii zajmowano się od bardzo dawna, stosując na przykład tzw. szyfry, np. szyfr Cezara. Na rys. 1.1 przedstawiono rozwój mechanizmów i systemów bezpieczeństwa. Rysunek ten dotyczy informacji rozumianej w sposób klasyczny, a od roku 1970 informacji dotyczącej systemów komputerowych.

Rysunek 1.1. Rozwój mechanizmów i systemów bezpieczeństwa

Szyfry stosowane w systemach komputerowych oparte zostały na rozwiązaniu firmy IBM. Rozwiązanie to zakładało, że algorytm szyfrowania jest jawny, natomiast tajny jest tzw. klucz. Wynikiem tych prac był standard DES, który zakładał tzw. symetryczny klucz służący do szyfrowania i deszyfrowania. Koncepcja ta pozwoliła zbudować kanał informacyjny (rys. 1.2), gdzie informacja była przesyłana w postaci zaszyfrowanej (kryptogram) kanałem bez zabezpieczeń, a kanałem bezpiecznym przesyłany był klucz.

Problem bezpiecznego przesyłania klucza pomiędzy nadawcą a odbiorcą, jest jednym z najważniejszych zagadnień współczesnej kryptografii. Aby poprawić bezpieczeństwo klucza, w latach 70-tych ubiegłego wieku

został opracowany algorytm szyfrowania niesymetrycznego RSA, w którym istnieją dwa klucze. Klucz publiczny jest ogólnie dostępny i służy do szyfrowania wiadomości, klucz prywatny jest chroniony i zazwyczaj nie występuje potrzeba jego przesyłania kanałem transmisji. Algorytm RSA bazuje na złożoności obliczeniowej faktoryzacji liczb pierwszych. Szyfry RSA bazują obecnie na kluczach 512 lub 1024 bitowych. Tak duże klucze wymagają dla brutalnego złamania bardzo dużo czasu. W roku 1994 Peter W. Shor opracował tzw. „algorytm Shora" umożliwiający odtwarzanie klucza prywatnego. Algorytm Shora przeznaczony jest wyłącznie dla niezrealizowanych fizycznie do dzisiaj komputerów kwantowych. Komputery kwantowe miałyby bazować na prawach mechaniki kwantowej i miałyby operować nie na liczbach, tylko na tzw. gęstości prawdopodobieństwa. Komputery kwantowe znajdowałyby w jednym przebiegu prawdopodobieństwo kilku liczb, które zostały użyte do wygenerowania klucza prywatnego. Taki komputer to w pewnym sensie przyszłość informatyki.



Rysunek 1.2. Klasyczny kanał informacyjny

Niezależnie od metod opartych o szyfrowanie i dystrybucję klucza, w monografii przedstawiono pewne metody uproszczone uwierzytelniania i podpisu. Do metod takich zalicza się np. stosowana w polskich urzędach metoda ePUAP. Wraz z podpisem elektronicznym są stosowane różne metody szyfrowania oraz różne metody certyfikacji. Aby rozwinąć owe zagadnienia, należy rozpocząć od przedstawienia koncepcji algorytmów kryptograficznych.

Książka ta jest przeznaczona dla inżynierów informatyków, jak również studentów kierunku Informatyka i innych kierunków nauk technicznych, w których wykorzystuje się zagadnienia bezpieczeństwa systemów komputerowych. Intencją książki jest przedstawienie wybranych zagadnień związanych z bezpieczeństwem sieci i systemów komputerowych oraz podniesienie świadomości czytelników na temat wagi tych problemów.