ROZDZIAŁ 2

Zrozumieć kryptografię

Wprowadzenie

W tym rozdziale wprowadzimy w podstawową terminologię oraz koncepcje kryptografii. Wprowadzenie to będzie miało nieformalny charakter i będzie stanowić zarys tak ogólny, jak to tylko możliwe.

Podstawowe koncepcje

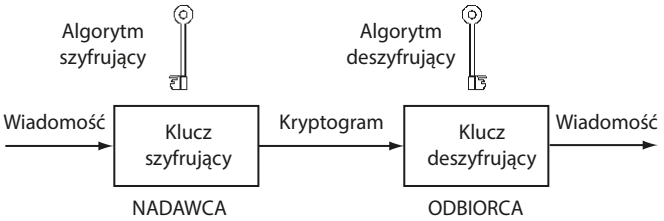
Idea systemu szyfrowania polega na tym, by ukryć poufną informację w taki sposób, aby jej znaczenie pozostało niezrozumiałe dla niepowołanych osób. Dwa najpowszechniejsze sposoby wykorzystania systemu szyfrowania to bezpieczne przechowywanie danych w pliku komputerowym oraz ich transmisja poprzez niezabezpieczone kanały takie jak Internet. W obu tych scenariuszach fakt, że dokument jest zaszyfrowany, nie uniemożliwia niepowołanym osobom uzyskania do niego dostępu, ale raczej gwarantuje, że nie będą one mogły zrozumieć tego, co widzą.

Informacja, która ma zostać ukryta, często jest nazywana *tekstem jawnym*, a operacja ukrywania nazywana jest *szyfrowaniem*. Zaszyfrowany tekst jawny to *szyfrogram* lub *kryptogram*, a zbiór zasad wykorzystanych do zaszyfrowania informacji w postaci tekstu jawnego to *algorytm szyfrujący*. Działanie tego algorytmu

zależy zwykle od *klucza szyfrującego*, stanowiącego wraz z wiadomością dane wejściowe algorytmu. Aby odbiorca mógł dotrzeć do wiadomości, musi istnieć *algorytm deszyfrujący*, który wraz z odpowiednim *kluczem deszyfrującym* pozwoli odtworzyć tekst jawny na podstawie szyfrogramu.

Ogólnie rzecz biorąc, zbiór zasad składających się na jeden z tych *algorytmów kryptograficznych* prawdopodobnie będzie bardzo skomplikowany i wymagać będzie starannego zaprojektowania. Dla celów tej książki czytelnik może je jednak uważać za „magiczne formuły", które za pomocą kluczy przekształcają informacje, nadając im niemożliwą do odczytania postać.

Poniższy rysunek obrazuje wykorzystanie *systemu szyfrowania* w celu ochrony przesyłanej wiadomości.



Każdy, kto przechwyci wiadomość w trakcie transmisji, nazywany jest *przechwytującym*. Inni autorzy stosują odmienne terminy, w tym takie jak „podsłuchiwacz", „wróg", „przeciwnik" czy nawet „ten zły". Trzeba jednak przyznać, że od czasu do czasu przechwytujący mogą być „tymi dobrymi" – więcej dowiemy się o nich nieco później. Nawet jeśli znają algorytm deszyfrujący, ogólnie rzecz biorąc, przechwytujący nie znają klucza deszyfrującego. To na tę lukę w ich wiedzy liczą ci, którzy chcą im uniemożliwić poznanie tekstu jawnego. *Kryptografia* jest dziedziną nauki zajmującą się projektowaniem systemów szyfrowania, podczas gdy *kryptoanaliza* to nazwa określająca proces dedukowania informacji o tekście jawnym na podstawie szyfrogramu, bez znajomości odpowiedniego

klucza. *Kryptologia* to zbiorczy termin, którym określa się zarówno kryptografię, jak i kryptoanalizę.

To bardzo ważne, by uzmysłowić sobie, że kryptoanaliza może nie być jedynym środkiem, za pomocą którego atakujący może uzyskać dostęp do tekstu jawnego.

Przypuśćmy na przykład, że ktoś przechowuje zaszyfrowane dane na swoim laptopie. Jasne jest, że ten ktoś musi mieć jakiś sposób na odzyskanie klucza deszyfrującego. Jeśli wiąże się to z zapisaniem go na kartce papieru przyklejonej na pokrywie laptopa, wtedy każdy, kto ukradnie laptopa, automatycznie wejdzie w posiadanie klucza deszyfrującego i nie będzie musiał uciekać się do kryptoanalizy. To tylko prosta ilustracja faktu, że zabezpieczenie danych polega na czymś więcej niż użycie dobrego algorytmu szyfrującego. W rzeczywistości, jak wielokrotnie podkreślaliśmy, bezpieczeństwo kluczy jest krytyczne dla bezpieczeństwa systemu kryptograficznego.

W praktyce większość ataków wykorzystujących kryptoanalizę próbuje ustalić klucz deszyfrujący. Jeśli się to powiedzie, wiedza napastnika będzie taka sama, jak wiedza zamierzonego odbiorcy i będzie on w stanie rozszyfrować całość komunikacji tak długo, jak długo klucze pozostaną niezmienione. W niektórych wypadkach napastnikowi może natomiast chodzić jedynie o odczytanie konkretnej wiadomości. Gdy inni autorzy mówią jednak, że jakiś algorytm został *złamany*, mają zwykle na myśli to, iż w praktyce napastnik znalazł sposób na uzyskanie klucza deszyfrującego[4].

Oczywiście napastnicy są w stanie złamać algorytm jedynie, jeśli dysponują wystarczającymi informacjami pozwalającymi na zidentyfikowanie właściwego klucza lub – częściej – zidentyfikowanie

[4] W literaturze kryptograficznej algorytm jest uznawany za złamany, jeśli pokazano atak, który zaprzecza założonym przez projektantów właściwościom bezpieczeństwa. Nie musi to być atak praktyczny i nie zawsze chodzi o odzyskanie klucza szyfrującego [przyp. kons. meryt.].

tych niewłaściwych. Ważne, by zdać sobie sprawę z tego, że ta dodatkowa informacja prawdopodobnie jest dla napastników kluczowa. Przypuśćmy na przykład, że wiedzą, iż tekst jawny jest po angielsku i odszyfrowanie jakiegoś szyfrogramu za pomocą odgadywanego klucza nie daje sensownego angielskojęzycznego tekstu jawnego. W tym wypadku wiadomo, że ten klucz nie może być poprawny.

Ważną kwestią, która po lekturze wprowadzenia powinna być już jasna, jest to, że znajomość klucza użytego do zaszyfrowania nie jest konieczna do odtworzenia wiadomości na bazie kryptogramu. Ta prosta konstatacja stanowi podstawę brzemiennego w skutki artykułu Diffiego i Hellmana. Miał on ogromny wpływ na współczesną kryptologię i zrodził naturalny podział na dwa typy systemów szyfrujących: symetryczne i asymetryczne.

System szyfrowania nazywany jest *konwencjonalnym* lub *symetrycznym*, jeśli na bazie klucza szyfrującego łatwo jest wydedukować klucz deszyfrujący. W praktyce w przypadku systemów symetrycznych te dwa klucze są często identyczne. Z tego powodu takie systemy można nazwać *systemami z kluczem tajnym* lub *systemami z jednym kluczem*. Jeśli jednak wydedukowanie klucza deszyfrującego na podstawie klucza szyfrującego jest praktycznie niemożliwe, system taki jest nazywany *asymetrycznym* lub *systemem z kluczem publicznym*. Pierwszy powód dla rozróżnienia tych dwóch typów systemów powinien być jasny. Jeśli chcemy przeszkodzić przechwytującemu, który zna algorytm, w uzyskaniu tekstu jawnego na podstawie przechwyconego szyfrogramu, niezbędne jest, by klucz deszyfrujący pozostał tajny. W wypadku systemu symetrycznego zmusza to do zachowania tajności również w kwestii klucza szyfrującego. Jeśli jednak system jest asymetryczny, znajomość klucza szyfrującego nie ma żadnego praktycznego znaczenia dla napastnika. W rzeczywistości klucz ten może być publicznie dostępny i zwykle faktycznie taki jest. W konsekwencji nadawca i odbiorca szyfrogramu nie muszą współdzielić żadnych tajemnic. Tak naprawdę nie muszą nawet sobie ufać.