omówiono określanie bezpieczeństwa kryptograficznego w taki sposób, że zarówno ma to solidne podstawy teoretyczne, jak i nadaje się do zastosowania w praktyce. Wyjaśniam pojęcia bezpieczeństwa informacyjnego obok bezpieczeństwa obliczeniowego, bezpieczeństwa bitowego obok kosztu pełnego ataku, bezpieczeństwa możliwego do udowodnienia obok bezpieczeństwa heurystycznego oraz generowania kluczy symetrycznych i niesymetrycznych. Rozdział ten kończą rzeczywiste przykłady błędów w mocnej na pozór kryptografii.

Definiowanie niemożliwego

W rozdziale 1 opisano bezpieczeństwo szyfru w odniesieniu do możliwości i celów napastnika, uznając go za bezpieczny, jeśli nie było możliwe osiągnięcie tych celów przez napastnika przy danych możliwościach. Ale co oznacza *niemożliwe* w tym kontekście?

Dwie rzeczy definiują pojęcie niemożliwości w kryptografii: bezpieczeństwo informacyjne oraz obliczeniowe. Z grubsza biorąc, *bezpieczeństwo informacyjne* dotyczy teoretycznego braku możliwości, a *bezpieczeństwo obliczeniowe* odnosi się do praktycznej niemożności. Bezpieczeństwo informacyjne nie mierzy bezpieczeństwa, ponieważ widzi szyfr jako bezpieczny lub nie, bez obszarów pośrednich; dlatego jest bezużyteczne w praktyce, mimo że odgrywa ważną rolę w kryptografii teoretycznej. Bezpieczeństwo obliczeniowe jest bardziej odpowiednią i praktyczną miarą siły szyfru.

Bezpieczeństwo w teorii — bezpieczeństwo informacyjne

Bezpieczeństwo informacyjne nie opiera się na tym, jak trudno jest złamać szyfr, lecz czy w ogóle istnieje taka ewentualność. Szyfr jest bezpieczny informacyjnie tylko wtedy, gdy nie można go złamać, nawet mając nieograniczony czas obliczania i pamięć. Jeśli nawet udany atak na szyfr zająłby biliony lat, taki szyfr *nie* jest bezpieczny informacyjnie.

Na przykład szyfr z hasłem jednorazowym, przedstawiony w rozdziale 1, jest bezpieczny informacyjnie. Przypomnijmy sobie, że szyfruje on jawny tekst P do postaci szyfrogramu $C = P \oplus K$, gdzie K jest losowym łańcuchem bitów, które są niepowtarzalne dla każdego tekstu jawnego. Szyfr ten jest bezpieczny informacyjnie, ponieważ mając szyfrogram i nieograniczony czas na wypróbowanie wszystkich możliwych kluczy K i wyznaczenie odpowiadającego mu tekstu jawnego P, nadal nie byłoby możliwe zidentyfikowanie prawidłowego K, ponieważ jest tyle możliwych P, ile K.

Bezpieczeństwo w praktyce — bezpieczeństwo obliczeniowe

W przeciwieństwie do bezpieczeństwa informacyjnego bezpieczeństwo obliczeniowe traktuje szyfr jako bezpieczny, jeśli nie można go złamać w *sensownym* czasie i za pomocą osiągalnych zasobów, takich jak pamięć, sprzęt, budżet, energia itp. Bezpieczeństwo obliczeniowe jest metodą określania bezpieczeństwa szyfru lub dowolnego algorytmu kryptograficznego.