3

BEZPIECZEŃSTWO KRYPTOGRAFICZNE

Kryptograficzne definicje bezpieczeństwa nie są takie same jak te ogólnie stosowane w bezpieczeństwie komputerów. Główna różnica między bezpieczeństwem oprogramowania a bezpieczeństwem kryptograficznym jest taka, że to drugie jest mierzalne. W przeciwieństwie do świata oprogramowania, gdzie aplikacje są zazwyczaj postrzegane jako bezpieczne lub nie, w świecie kryptografii często możliwe jest obliczenie rozmiaru wysiłku potrzebnego do złamania algorytmu kryptograficznego. Ponadto, gdy bezpieczeństwo oprogramowania skupia się na uniemożliwianiu napastnikom nadużywania kodu programu, celem bezpieczeństwa kryptograficznego jest zapewnienie, aby dobrze zdefiniowane problemy były niemożliwe do rozwiązania.

Problemy kryptograficzne obejmują pojęcia matematyczne, jednak nie skomplikowaną matematykę – przynajmniej nie w tej książce. Ten rozdział prowadzi nas przez kilka z tych pojęć bezpieczeństwa i to, jak są one stosowane do rozwiązywania rzeczywistych problemów. W poniższych punktach