używanych przez miliony, a obejmujących telefony komórkowe, Wi-Fi oraz inteligentne karty transportu publicznego. Ale to już historia. Na szczęście, mimo że zajęło to 20 lat, wiemy teraz, jak projektować bezpieczne szyfry strumieniowe, i wierzymy, że chronią takie elementy, jak połączenia Bluetooth, mobilne połączenia 4G, połączenia TLS i wiele innych.

W tym rozdziale pokazano, jak działają szyfry strumieniowe, i omówiono dwie główne ich klasy: szyfry stanowe oraz szyfry oparte na liczniku.

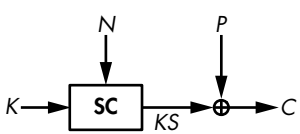
Następnie przyjrzymy się szyfrom strumieniowym zorientowanym na oprogramowanie oraz na sprzęt i kilku szyfrom, które nie są bezpieczne (takim jak A5/1 w GSM łączności mobilnej oraz RC4 w TLS) oraz kilku najnowocześniejszym bezpiecznym szyfrom (takim jak Grain-128a dla sprzętu oraz Salsa20 dla oprogramowania).

Jak działają szyfry strumieniowe

Szyfry strumieniowe bardziej przypominają deterministyczne generatory bitów losowych (DRBG) niż dojrzałe generatory liczb pseudolosowych (PRNG), ponieważ podobnie jak DRBG, szyfry strumieniowe są deterministyczne. Ich determinizm pozwala odszyfrowywać je poprzez odtwarzanie bitów pseudolosowych używanych do szyfrowania. Korzystając z PRNG, można by zaszyfrować, lecz nigdy nie odszyfrować – co jest bezpieczne, lecz bezużyteczne.

To, co różni szyfry strumieniowe od generatorów DRBG, to fakt, że te ostatnie przyjmują jedną wartość wejściową, natomiast szyfry strumieniowe – dwie: klucz i wartość jednorazową. Klucz powinien być tajny i ma zazwyczaj 128 lub 256 bitów. Wartość jednorazowa nie musi być wartością tajną, lecz powinna być niepowtarzalna dla każdego klucza i zwykle ma między 64 a 128 bitów.

Szyfry strumieniowe tworzą pseudolosowy strumień bitów nazywany *strumieniem klucza* (*keystream*). Aby zaszyfrować tekst, strumień klucza i tekst jawny podlegają działaniu XOR, a na szyfrogramie wykonuje się XOR, aby go odszyfrować. Na rysunku 5.1 pokazano podstawowe szyfrowanie szyfrem strumieniowym, gdzie **SC** jest algorytmem szyfru strumieniowego, *KS* jest strumieniem klucza, *P* jest tekstem jawnym, a *C* szyfrogramem.



Rysunek 5.1. Jak szyfruje szyfr strumieniowy, biorąc tajny klucz K i publiczną wartość jednorazową N

Szyfr strumieniowy oblicza $KS = \mathbf{SC}(K, N)$, szyfruje jako $C = P \oplus KS$ i odszyfrowuje jako $P = C \oplus KS$. Funkcje szyfrowania i odszyfrowywania są takie same, ponieważ obie robią to samo, a mianowicie wykonują działanie XOR na bitach oraz strumieniu klucza. Z tego powodu na przykład niektóre biblioteki kryptograficzne dostarczają jedną funkcję `encrypt`, która służy zarówno do szyfrowania, jak i odszyfrowywania.

Szyfry strumieniowe pozwalają szyfrować komunikat za pomocą klucza K_1 i wartości jednorazowej N_1, a następnie szyfrują inny komunikat przy użyciu klucza K_1 i wartości jednorazowej N_2, różniącej się od N_1, lub za pomocą