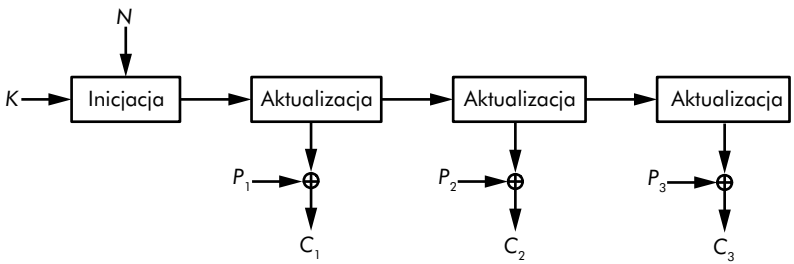
klucza K_2, różniącego się od K_1 i N_1. Nie należy jednak nigdy szyfrować ponownie za pomocą K_1 i N_1, ponieważ byłoby to użycie tego samego strumienia klucza *KS*. Mielibyśmy wtedy pierwszy szyfrogram $C_1 = P_1 \oplus KS$, drugi szyfrogram $C_2 = P_2 \oplus KS$, a znając P_1, można by określić $P_2 = C_1 \oplus C_2 \oplus P_1$.

Uwaga *Wartość jednorazowa, w języku angielskiem jest nazywana słowem nonce, co jest skrótem od number used only once (liczba użyta tylko raz). W kontekście szyfrów strumieniowych jest czasami określana jako IV (od initial value, czyli wartość początkowa).*

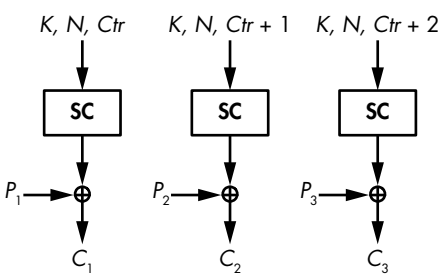
Szyfry strumieniowe stanowe i oparte na liczniku

Z ogólnej perspektywy są dwa typy szyfrów strumieniowych: stanowe i oparte na liczniku. *Szyfry strumieniowe stanowe* (*stateful stream ciphers*) mają tajny stan wewnętrzny, który ewoluuje podczas generowania strumienia klucza. Szyfr inicjalizuje stan z klucza i wartość jednorazową, a następnie wywołuje funkcję aktualizacji, aby zaktualizować wartość stanu, i tworzy jeden lub więcej bitów strumienia klucza ze stanu, jak to pokazano na rysunku 5.2. Na przykład słynny RC4 jest szyfrem stanowym.



Rysunek 5.2. Stanowy szyfr strumieniowy

Szyfry strumieniowe oparte na liczniku (*counter-based stream ciphers*) tworzą fragmenty strumienia klucza z klucza, wartości jednorazowej oraz wartości licznika, jak to pokazano na rysunku 5.3. Inaczej niż w stanowych szyfrach strumieniowych, takich jak Salsa20, żaden tajny stan nie jest zapamiętywany podczas generowania strumienia klucza.



Rysunek 5.3. Szyfr strumieniowy oparty na liczniku