Odpowiedzi na pytania

1. Jak działa AES?

   AES jest blokowym szyfrem symetrycznym operującym na blokach 128 bitów. Klucz ma długość 128, 192 lub 256 bitów. Szyfrowanie przebiega w rundach.

   Każda runda składa się z:
   - SubBytes – nieliniowa zamiana S-box.
   - ShiftRows – przesunięcia wierszy.
   - MixColumns – mieszanie kolumn.
   - AddRoundKey – XOR z kluczem rundowym.

2. Konfuzja i dyfuzja
   Konfuzja to zaciemnianie zależności między kluczem a szyfrogramem. Dyfuzja to rozpraszanie wpływu bitów wejścia po wielu bitach wyjścia.
   • Konfuzję w AES zapewnia SubBytes (S-box).
   • Dyfuzję zapewniają ShiftRows oraz MixColumns.

3. Szyfry blokowe i strumienioweSzyfry blokowe działają na stałych blokach (np. 128 bitów) i wymagają trybów pracy. Przykład: AES.Szyfry strumieniowe generują keystream i XORują go z danymi. Mogą działać bit po bicie. Przykład: ChaCha20.