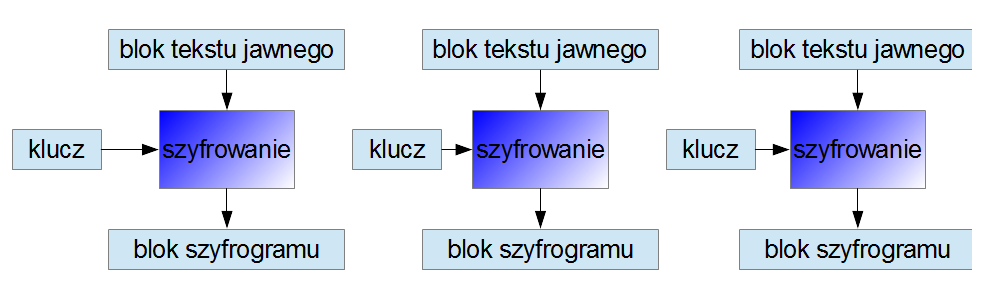
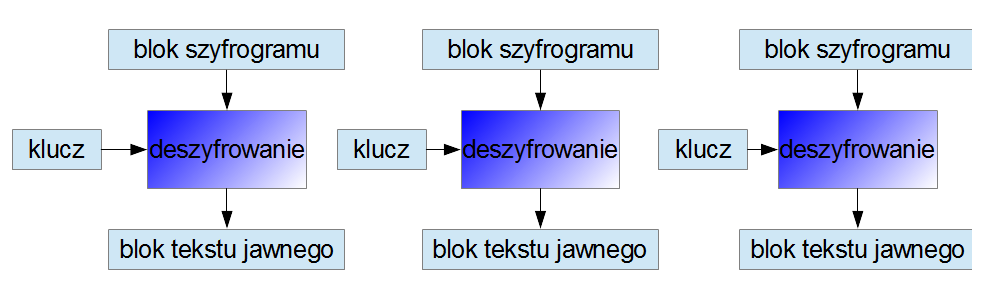
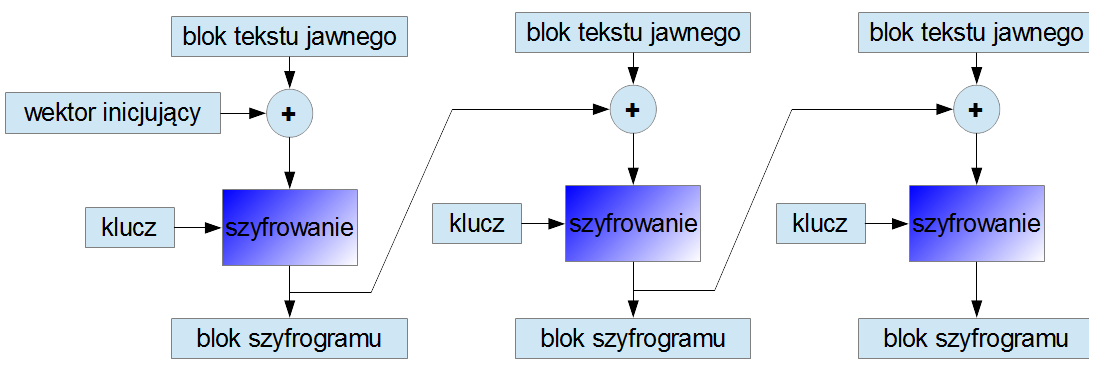
**Pytanie 1:**

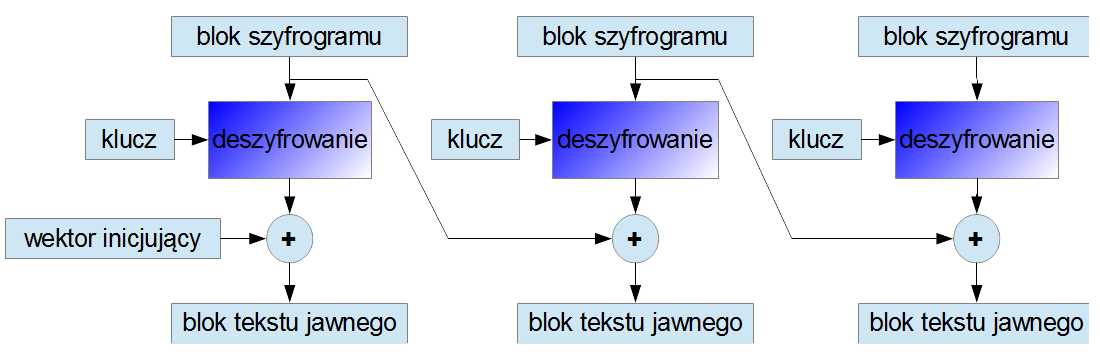
**CEB:**



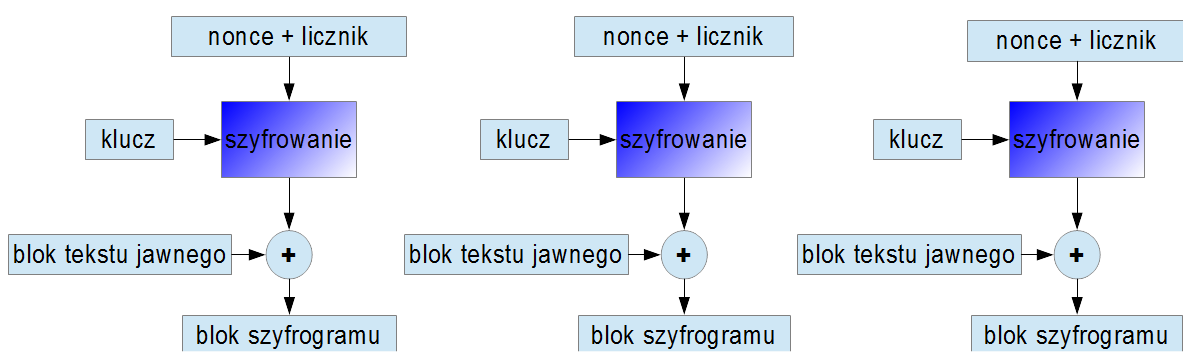


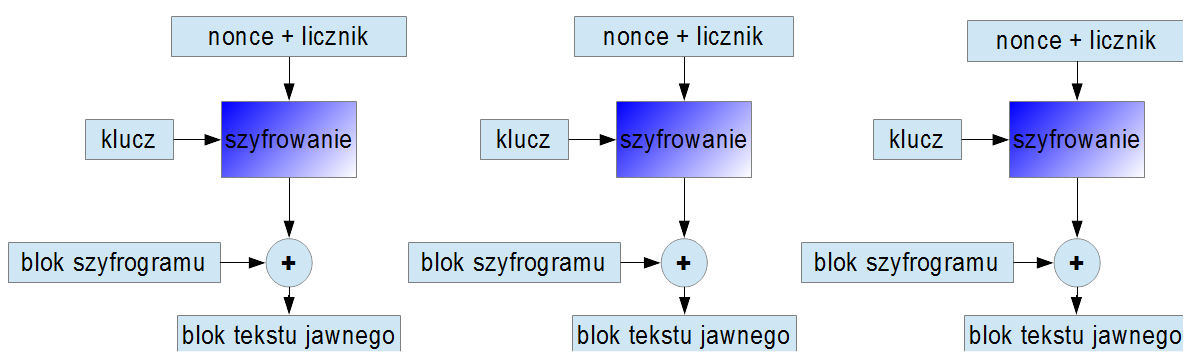
**CBC:**





**CRT:**





Źródła schematów: <http://www.crypto-it.net/pl/teoria/tryby-szyfrow-blokowych.html>

**Pytanie2:**

Można stosować szyfrowanie kluczy oraz haseł, ponadto unikać udostępniania kodu w całości użytkownikowi oraz ograniczać informację na temat działania programu w celu ochrony przez dezasemblacją kodu. Ponadto jedną z metod ochrony jest tgz. zaciemnianie kodu, można je osiągnąć poprzez:

* Transformację wyglądu (zmiana nazw identyfikatorów , zmiana formatowania , usunięcie komentarzy)
* Transformację kontroli (zmiana przebiegu, rozszerzenie warunków pętli, zmiana kolejności pętli/ wyrażeń itp, klonowanie metod)
* Transformację danych (zmiana kodowania, zmiana długości życia zmiennej , rozdzielenie zmiennych , zmiana relacji dziedziczenia)

**Pytanie3:**Porównania szybkości działania bibliotek można dokonać przy pomocy sprawdzenia czasu wykonywania identycznego zadania przez poszczególne biblioteki. Ja jednak tego nie dokonałam.

**Pytanie4:**dla biblioteki PyCrypto: <https://www.cvedetails.com/cve/CVE-2012-3458/>  
ponadto strona <https://nvd.nist.gov/vuln>

**Pytanie5:**Wynika to z faktu, że środowisku JDK zostało odgórnie nałożone ograniczenie dotyczące długości klucza. Jest to powiązane z restrykcjami w niektórych krajach dotyczącymi dopuszczalnej wielkości (siły) klucza.

**Pytanie6:**

Tryb CRT oraz CBC daje większe bezpieczeństwo niż ECB. Aczkolwiek należy zmieniać klucz co kilka wysyłanych wiadomości, aby mieć pewność że wiadomości nie zostaną odszyfrowane.