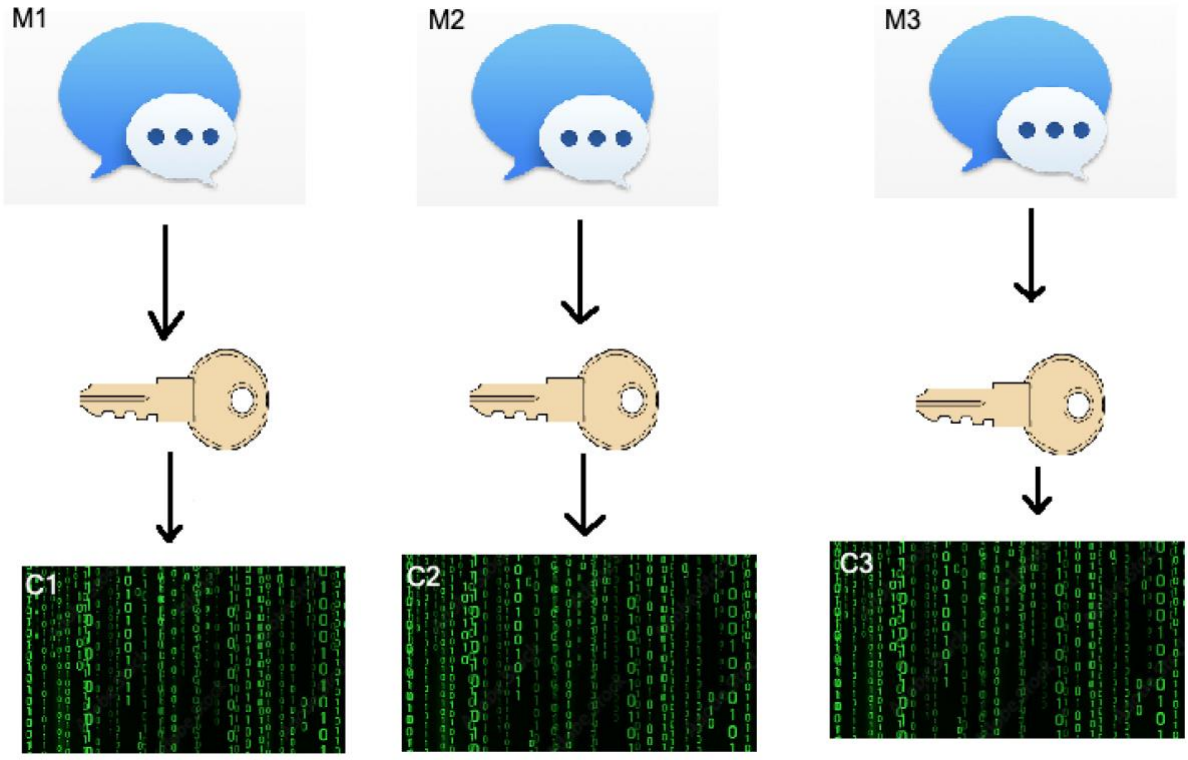
E-media, Projekt nr 2

Szyfrowanie blokowe:

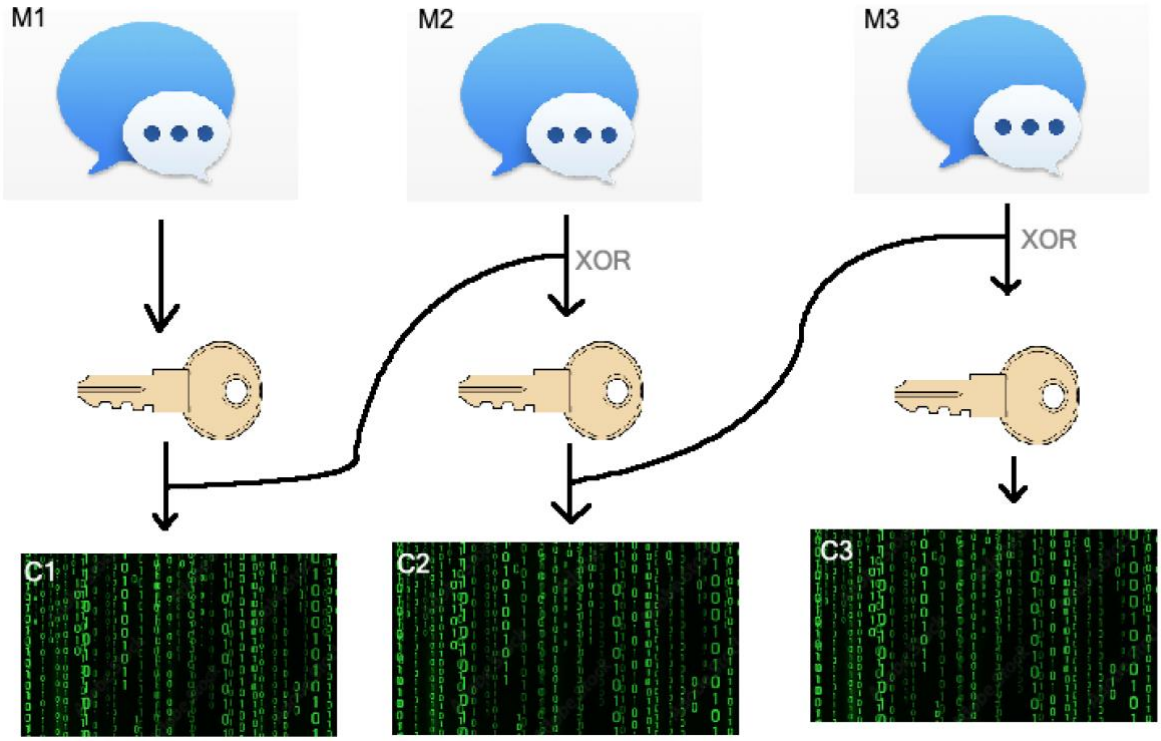
- ECB [electronic codebook]



Zalety: szybkość szyfrowania i deszyfrowania, możliwe wykonywanie operacji na kilku blokach na raz, możemy odszyfrować dowolny blok w dowolnym momencie, podczas błędu w transmisji tylko jeden blok będzie do naprawy.

Wady: tak samo szyfrowane są identyczne bloki wiadomości, w ogóle nie jest bezpieczny.

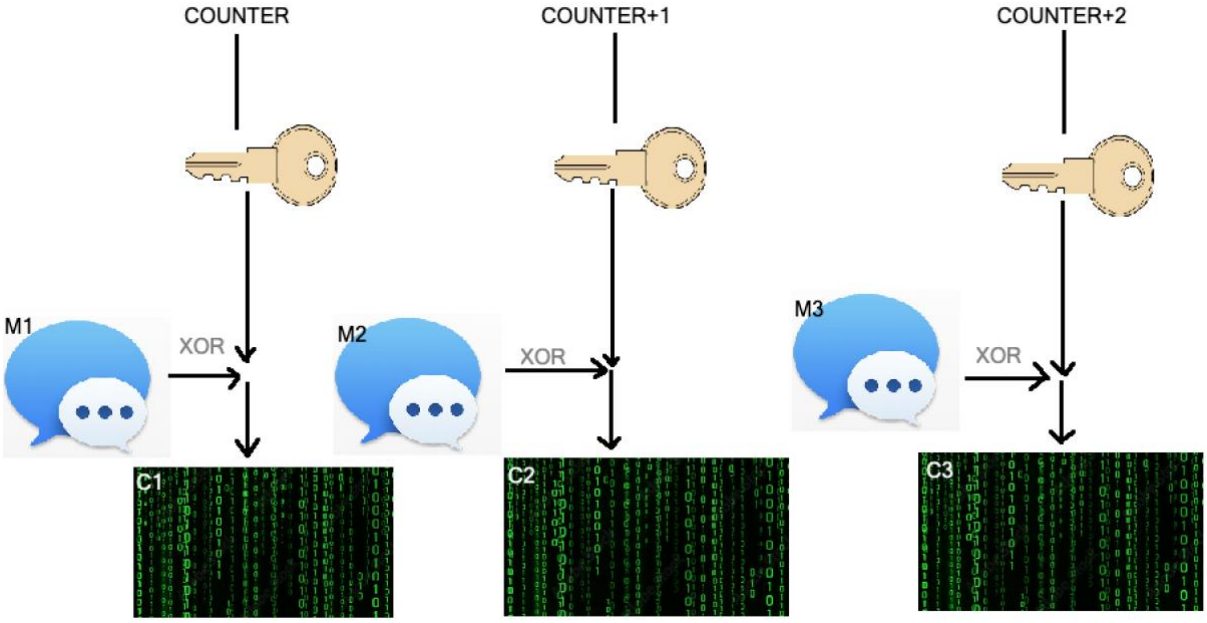
- CBC [Cipher block chaining]



Zalety: Poprzez łańcuchowe łączenie zaszyfrowanej wiadomości z następną wiadomością do zaszyfrowania (XOR), każdy zaszyfrowany blok będzie różny (naprawia problem ECB)

Wady: Wolniejsze rozwiązanie (musimy czekać na zaszyfrowanie poprzednich bloków). Gdy podczas szyfrowania jednej wiadomości coś się zepsuje, następny blok może być przekłamany (tracimy dwa bloki) i musimy zacząć od nowa.

- CTR [counter]– (nie blokowy) Za każdym następnym blokiem zwiększamy licznik ustalony na początku i jego szyfrujemy, a następnie Xorujemy z wiadomością.



Zalety: szybki, bezpieczny, nie potrzeba operacji dekrypcji do odszyfrowania wiadomości, tylko szyfrujemy ponownie klucz

Wady: Nie można używać drugi raz tego samego licznika. Bez odpowiednich zabezpieczeń można przekłamać wiadomość zaszyfrowaną