Zaawansowane zagadnienia bezpieczeństwa - dowodliwe bezpieczeństwo, zadania treningowe na 9.11.2010

1. Rozważmy losowe błądzenie po hiperkostce. W każdym kroku:

   - wybieramy losowo jedną z $\log n$ współrzędnych,
   - zmieniamy wartość na tej współrzędnej (tzn. jeśli był tam bit b to zmieniamy wartość współrzędnej na bit przeciwny $1 - b$) — inaczej interpretując poruszamy się po krawędzi wyznaczonej przez tę współrzędną.

   Za pomocą couplingu można starać się pokazać, że po pewnej liczbie kroków zbliżymy się do rozkładu jednostajnego.

   Pytanie: **dlaczego dla wskazanego procesu nie uda się to? czy jest to tylko problem z techniką dowodową, czy przyczyny są głębsze?**

2. Rozważmy losowe mieszanie n wiadomości. W każdym kroku procesu:

   - wybieramy losowy podzbiór $n/2$ wiadomości i ustawiamy je na pierwszych $n/2$ pozycjach po losowym spermutowaniu;
   - pozostałe $n/2$ wiadomości umieszczamy na pozycjach od $n/2 + 1$ do n z zachowaniem ich orginalnej kolejności.

   Ile kroków potrzeba, aby w ten sposób zbliżyć się na odległość $1/1000$ **(wg *total variation distance*) do rozkładu jednostajnego wśród permutacji na** n **elementach?**