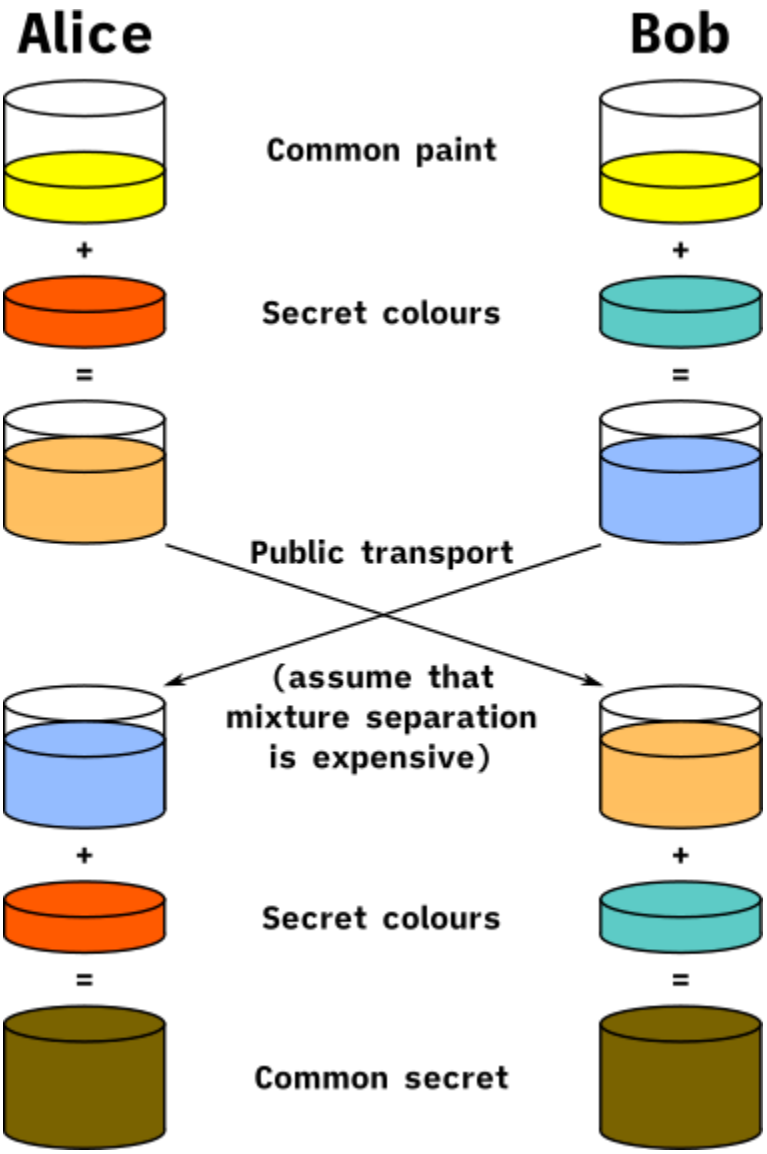
Protokół Diffiego-Hellmana

Protokół Diffiego-Hellmana służy do ustalenia wspólnego tajnego klucza przy użyciu publicznych środków komunikacji. Następujący diagram przedstawia ogólną ideę uzgodnienia klucza na przykładzie kolorów zamiast liczb. Kluczowe dla procesu jest to, że Alicja i Bob używają jedynie prostej operacji mieszania kolorów. Operacja ta powinna być możliwie trudna do odwrócenia (być funkcją jednokierunkową). Wygenerowany klucz jest praktycznie niemożliwy do odtworzenia przez osobę podsłuchującą. Kolor żółty jest znany Alicji i Bobowi:



Weryfikację obliczeniową poprawności klucza wygenerowanego w p. 2 ćwiczenia.

1. p = 17, g = 3 (1 < g < p)

2. A secret = 10
3. B secret = 16
4. A shared key = g ^ x mod p = 3 ^ 10 mod 17 = 8
5. B shared key = g ^ y mod p = 3 ^ 16 mod 17 = 1
6. Wymiana shared keys
7. Session key:
8. Dla A: B ^ x mod p = 1 ^ 10 mod 17 = 1
9. Dla B: A ^ y mod p = 8 ^ 16 mod 17 = 1

Wnioski

- protokół DH jest bardzo prosty w implementacji
- protokół DH może służyć do ustalenia wspólnego klucza dla kryptografii symetrycznej
- jest odporny na podsłuchanie przy ustalaniu wspólnego klucza
- nie jest odporny na Man-in-the-Middle attack