

Security: Diffie Hellman

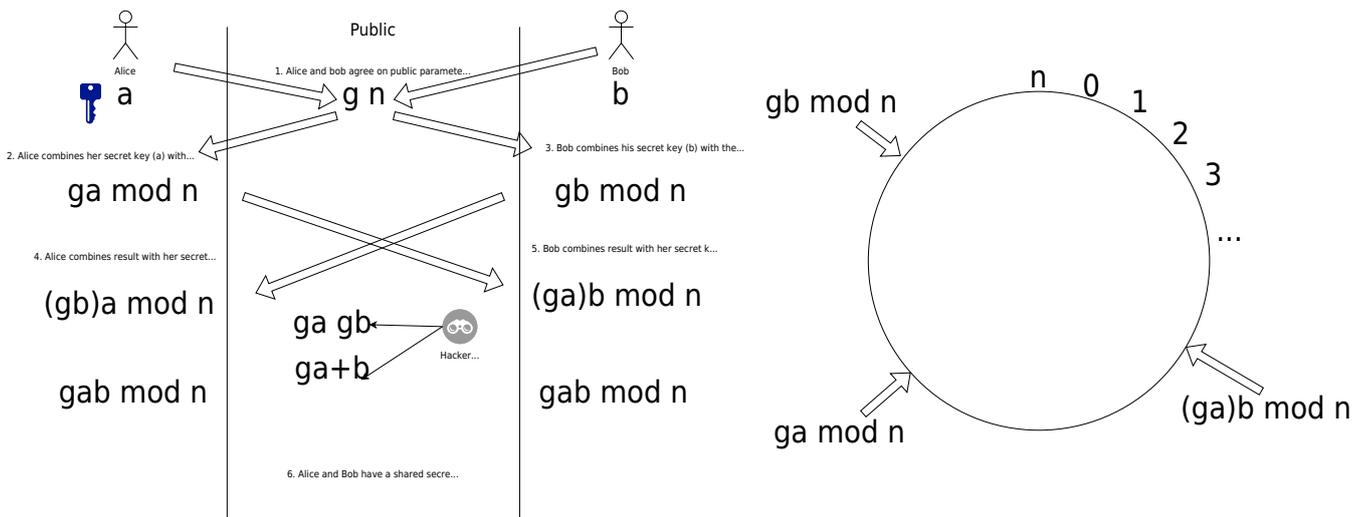
źródła:



https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

Schemat

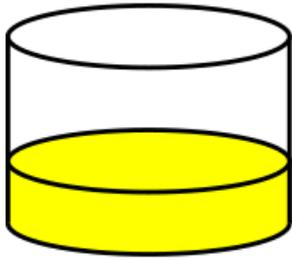
Diffie-Hellman key exchange



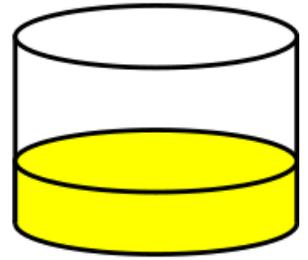
Author: Kacper Ostrowski

Alice

Bob

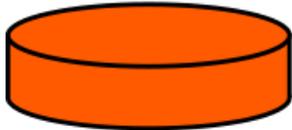


Common paint

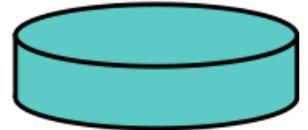


+

+

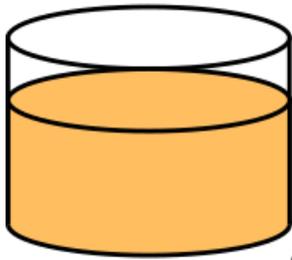


Secret colours

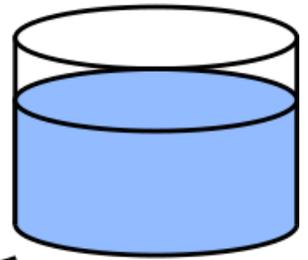


=

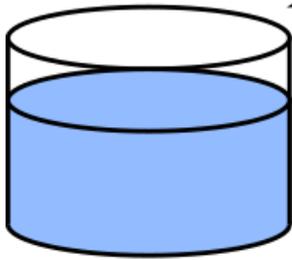
=



Public transport



(assume that mixture separation is expensive)

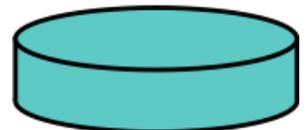


+

+

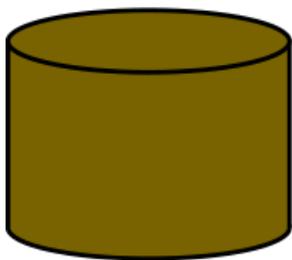


Secret colours

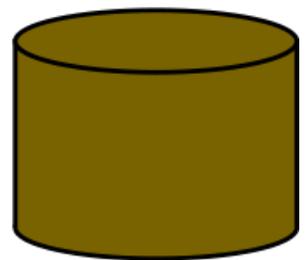


=

=



Common secret



From:

<https://wiki.ostrowski.net.pl/> - **Kacper's Wiki**

Permanent link:

https://wiki.ostrowski.net.pl/doku.php?id=notatki:diffie_hellman&rev=1747833803

Last update: **2025/05/21 15:23**