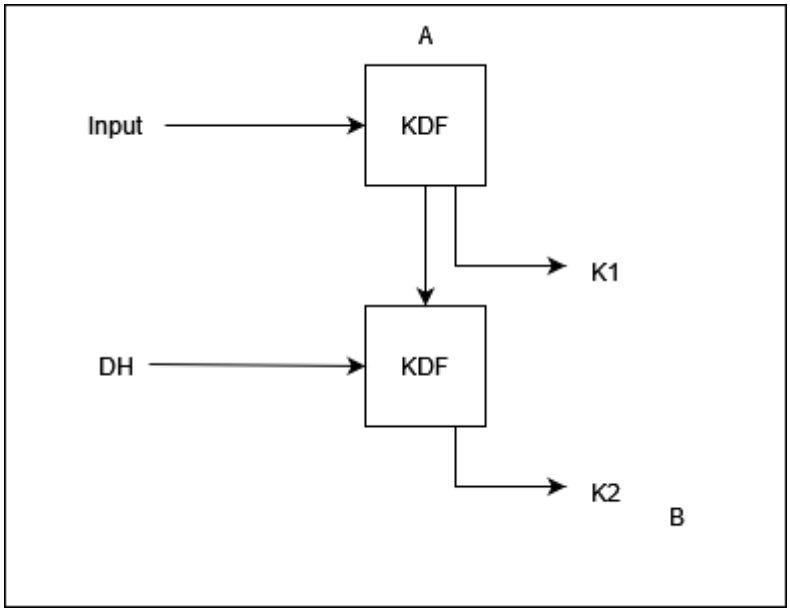
Double Rachet

Similar a una función hash, se mete una semilla y a partir de un KDF se genera otro KDF. Estos KDF generan claves. Para reforzar esto en uno de los KDF se cambia la semilla por un Diffie-Helman. Tenemos una cadena de recepción y una de envío. K1 se utiliza para cifrar los mensajes enviados a un usuario B (Es una cadena de envío). B es una cadena de recepción.



En un sentido se puede generar la secuencia, pero no se puede volver para atrás obteniendo una de las claves. Normalmente se tiene un rachet para la cadena de envío y otro para la recepción.