№5 A послал B сообщение m в формате $(\mathcal{E}_B(m), A)$. $D_i(\mathcal{E}_i(m)) = m$

Пусть пользователь C хочет перехватить $(\mathcal{E}_B(m), A)$ и также послать его в верном формате C

Это означает, что когда пользователь C перехватывает сообщение $(\mathcal{E}_B(m), A)$, то он преобразует его в новое сообщение того же формата, т.е. в сообщение $(\mathcal{E}_B(m), C)$ и затем отправляет его B.

Пользователь B, в свою очередь, получив $\mathcal{E}_B(m)$, расшифровывает его с помощью D_B:

$$D_B(\mathcal{E}_B(m)) = m$$

Затем B отправляет сообщение C в формате $(\mathcal{E}_C(m), B)$.

Пользователь C, получив $\mathcal{E}_C(m)$, расшифровывает его с помощью D_C:

$$D_C(\mathcal{E}_C(m)) = m.$$