Q.6 Show that Alice and Bob outputs the same key.

Alice outputs K & Bob outputs $w \oplus t$.

Here, we need to show that $K = w \oplus t$.

$$
\begin{aligned}
& w \oplus t \\
= \; & u \oplus r \oplus t \\
= \; & s \oplus t \oplus r \oplus t \\
= \; & s \oplus r \qquad [\because \; t \oplus t = 0] \\
= \; & K \oplus r \oplus r \\
= \; & K \qquad [\because \; r \oplus r = 0]
\end{aligned}
$$

So, it is proved that $K = w \oplus t$.

Bob & Alice both outputs the same key.

(2). Here, s, u & w are public. Because, they are sent over a public ~~co~~ communicati- Channel.

From Slide 343, we can say that everything is known to adversary except the messages generated randomly & uniformly.

In our case, K, r, t are generated uniformly.

So. $\boxed{s, u \text{ \& } w \text{ are public messages.}}$

(3). It is possible to reconstruct the key using public messages. [s, u & w

$$u \oplus w \oplus s$$

$$= s \oplus t \oplus w \oplus s$$

$$= t \oplus w \qquad [\because s \oplus s = 0]$$

We know from part (1) that $w \oplus t$ is a key. And is generated using public messages u, w, s.