Q.5 Show that is possible to find a message m such that we can forge a valid signature if we know that the scheme chooses the secret random value e to be the same as the signing exponent s (that is, $e = s$ in the scheme).

$\Rightarrow$ Suppose a message $m = 0$, which is valid because $0 \leq m < q$

$e = s$.

So, $s_1 \equiv [g^e \pmod p] \pmod q$

$\equiv [g^s \pmod p] \pmod q$

$\equiv v \pmod q$. [slide 437]

We know v & q are public.

So, s_1 can be known easily using above method.

$s_2 \equiv (m + ss_1) e^{-1} \pmod q$

$\equiv (0 + ss_1) e^{-1} \pmod q$ [$\because m = 0$]

$\equiv ss_1 s^{-1} \pmod q$ [$\because e = s$]

$\equiv s_1 \pmod q$ [$\because ss^{-1} \equiv 1 \pmod q$]

Here, s_1 is known for given value of e & m. q is also public.

So, s_2 can be figured out easily.

Overall, it is proved that if $e = s$, for a message $m = 0$, a valid signature can be forged easily with publicly available information.