Solution to daily post due October 30th (Crypto Fall 2020)

Suppose that Alice signs two messages (m_1, R, s_1) and (m_2, R, s_2). Since you see the same R, you know she used the same k. Here I explain how this leads to an attack: you can obtain the re-used k and then Alice's secret key.

1. **Obtaining** k. Since R is the same, $x = x(R)$ is the same. We have

$$s_1 \equiv k^{-1}(m_1 - ax) \pmod{n}, \quad s_2 \equiv k^{-1}(m_2 - ax) \pmod{n}.$$

   We can combine these two equations, to obtain

$$s_1 - s_2 \equiv k^{-1}(m_1 - m_2) \pmod{n}.$$

   Rearranging this, we have

$$k(s_1 - s_2) \equiv m_1 - m_2 \pmod{n}.$$

   The values $s_1 - s_2$ and $m_1 - m_2$ are known. So in the unknown k, this is a linear congruence. That is, we can solve it using the Euclidean algorithm. It will probably have only one solution, if $s_1 - s_2$ is coprime to n (we would typically take n to be prime). But even if it has several solutions, that's not too big a deal, we can just carry them forward to what follows.

2. **Obtaining** a. We can rearrange the standard equations to get

$$m_1 - s_1 k \equiv ax \pmod{n}$$

   In this, we know $m_1 - s_1 k$ and x, so we again have a linear congruence in the unknown a. Again, we solve this to obtain a. If we have several k, we can do this for each one. We can always test which a is correct by checking if aP is Alice's public key or not. If we get several a (in the case n is not prime) we could also check those.