Exercise 1

Given: DSA, Group g, order q, generator g, secret key x, parameter p $R = (g^r \mod p) \mod q$

$X = g^x \mod p$ 2 Pairs: (m, R, s) and (m', R, s') find x

pk = (G, q, g, X)

$s = \frac{H(m)+x \cdot R)}{r} \mod q$

So the attacker as the two Pairs and pk.

The attacker can make the equation

$$s - s' = (r^-1 \cdot (H(m) + x \cdot R)) \mod q - (r^{-1} \cdot (H(m') + x \cdot R)) \mod q$$

This means we can wrap the mod around the whole right term

The inner right is:

$$r^{-1} \cdot (H(m) + x \cdot R) - r^{-1} * H(m') + x \cdot R)$$

which is

$r^{-1} * (H(m) - H(m'))$

which makes:

$$s - s' = (r^{-1} \cdot (H(m) - H(m'))) \mod q$$

if $H(m) - H(m') < q$ the solution is very obvious, as r is also smaller than q.

In that case we can just get rid of mod q. If this is however not the case we need to try a bit.