Volga CTF Quals 2016 - Lazy

Yana Permana

March 27, 2016

Known
r, s_1, s_2, h_1, h_2

$s_1 = \frac{h_1 + x \cdot r}{k} \bmod q$

$s_2 = \frac{h_2 + x \cdot r}{k} \bmod q$

Unknown
k, x

Asked
k, x

Solve
The first thing to do is find k

Because $x \cdot k$ is exist in each equation, we can eliminate it and the equation become like this

$s_1 = \frac{h_1}{k} \bmod q$

$s_2 = \frac{h_2}{k} \bmod q$

Let's combine these two equations into one equation

$s_1 - s_2 = (\frac{h_1}{k}) - (\frac{h_2}{k}) \bmod q$

Simplify

$s_1 - s_2 = \frac{h_1 - h_2}{k} \bmod q$

Exchange $s_1 - s_2$ w/ k so become like this

$k = \frac{h_1 - h_2}{s_1 - s_2} \bmod q$

After k known, let's find x by the following equation:

$x = -\frac{s_2 \cdot h_1 - s_1 \cdot h_2}{r \cdot (s_2 - s_1)} \bmod q$

For this equation, I have not been able to prove it.

You can see this equation in a paper entitled "The Security of DSA and ECDSA: Bypassing the Standard Elliptic Curve Certification Scheme" by Serge Vaudenay.