

According to the decompilation of the Ciso Vigenere hash algorithm, when the password length is less than 16 the idea behind Ciso Vigenere hash algorithm is:

Let  $p$  be the password that the user types.

Let  $hp$  be the hardcoded password in the code of Packet Tracer.

Let  $lp$  be the length of the user input password.

Let  $h$  be the hash value obtained from the custom algorithm.

So that:

$$\begin{aligned}
& \forall h \forall lp \forall hp [hp = \\
& ((d, s, f, d, :, k, f, o, A, , , i, y, e, w, r, k, l, d, J, K, D, H, S, U, B, s, g, v, c, a, 6, 9, 8, 3, 4, n, c, x, v), \\
& 0 < lp < 16, \\
& h_0 = 0, \\
& h_1 = 8, \\
& h = \\
& \Sigma_{i=2}^{lp} \begin{cases} ((p_i \oplus hp_{8+i}) \gg 4) + 0x30, & \text{if } (p_i \oplus hp_{i+8} \wedge 0xffffffff0 < 0xa0) \text{ and if } i \equiv 0 \pmod{2} \\ ((p_i \oplus hp_{8+i}) \gg 4) + 0x37, & \text{if } (p_i \oplus hp_{i+8} \wedge 0xffffffff0 \geq 0xa0) \text{ and if } i \equiv 0 \pmod{2} \\ ((p_i \oplus hp_{8+i}) \wedge 0xf) + 0x30, & \text{if } (p_i \oplus hp_{i+8} \wedge 0xf < 0x0a) \text{ and if } i \equiv 1 \pmod{2} \\ ((p_i \oplus hp_{8+i}) \wedge 0xf) + 0x37, & \text{if } (p_i \oplus hp_{i+8} \wedge 0xf \geq 0x0a) \text{ and if } i \equiv 1 \pmod{2} \end{cases} \\
& ) \implies \#p[p = \mathbf{rev}(h)] \\
& (0)
\end{aligned}$$