Sistemas Computacionales

Lenguaje Ensamblador

Avances de Proyecto

Implementación de algoritmo de salsa20

Einar Naim Aguilar Santana

Daniel Alejandro Barbosa Ayala

Axel Daniel Macias Heredia

Sebastian Rodriguez Hernandez

Jesús Ruvalcaba Lozano

Durante la semana de 22 de mayo a 26 de mayo de 2023 se avanzo con respecto al cronograma ya que se implementó a función Quarterround Function.

Su finalidad de es mezclar y transformar los datos en bloques de 32 bits.

Quarterround es un componente clave en el algoritmo, que se utiliza en aplicaciones de seguridad. Proporciona una capa adicional de seguridad al aplicar una serie de operaciones aritméticas y de bits a los datos.

$$
\begin{aligned}
&\text{quarterround}(\texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}) \\
&\qquad = (\texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}). \\
&\text{quarterround}(\texttt{0x00000001}, \texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}) \\
&\qquad = (\texttt{0x08008145}, \texttt{0x00000080}, \texttt{0x00010200}, \texttt{0x20500000}). \\
&\text{quarterround}(\texttt{0x00000000}, \texttt{0x00000001}, \texttt{0x00000000}, \texttt{0x00000000}) \\
&\qquad = (\texttt{0x88000100}, \texttt{0x00000001}, \texttt{0x00000200}, \texttt{0x00402000}). \\
&\text{quarterround}(\texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000001}, \texttt{0x00000000}) \\
&\qquad = (\texttt{0x80040000}, \texttt{0x00000000}, \texttt{0x00000001}, \texttt{0x00002000}). \\
&\text{quarterround}(\texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000000}, \texttt{0x00000001}) \\
&\qquad = (\texttt{0x00048044}, \texttt{0x00000080}, \texttt{0x00010000}, \texttt{0x20100001}). \\
&\text{quarterround}(\texttt{0xe7e8c006}, \texttt{0xc4f9417d}, \texttt{0x6479b4b2}, \texttt{0x68c67137}) \\
&\qquad = (\texttt{0xe876d72b}, \texttt{0x9361dfd5}, \texttt{0xf1460244}, \texttt{0x948541a3}). \\
&\text{quarterround}(\texttt{0xd3917c5b}, \texttt{0x55f1c407}, \texttt{0x52a58a7a}, \texttt{0x8f887a3b}) \\
&\qquad = (\texttt{0x3e2f308c}, \texttt{0xd90a8f36}, \texttt{0x6ab2a923}, \texttt{0x2883524c}).
\end{aligned}
$$