Exercise_5

1.

$$
\begin{aligned}
ab &= x(2^n+1)+y \\
&= x*2^n+x+y \\
|y| &< 2^n+1
\end{aligned}
$$

so there are two situations:

1) y $\geq$ 0

$$
\begin{aligned}
ab \mod 2^n+1 &= y \\
ab \mod 2^n+1 &= ab \mod 2^n - ab|2^n \\
&= x+y-x \\
&= y
\end{aligned}
$$

Proved.

2) y < 0

$$
\begin{aligned}
ab \mod 2^n+1 &= (x-1)(2^n+1)+2^n+1-y \mod 2^n+1 \\
&= 2^n+1-y \\
ab \mod 2^n+1 &= ab \mod 2^n - ab|2^n + 2^n + 1 \\
&= x+y-x+2^n+1 \\
&= 2^n+1-y
\end{aligned}
$$

Proved.

2.

The input is X_1, X_2, X_3, X_4, and the output is Y_1, Y_2, Y_3, Y_4.

We have to prove that

$$
X_1, X_2, X_3, X_4 = In(Y_1, Y_2, Y_3, Y_4)
$$

We have

$$
\begin{cases}
Y_1 = X_1 \oplus X_5 \\
Y_2 = X_2 \oplus X_6 \\
Y_3 = X_3 \oplus X_5 \\
Y_4 = X_4 \oplus X_6 \\
X_5, X_6 = MA(X_1 \oplus X_3, X_2 \oplus X_4)
\end{cases}
$$

So

$$\begin{gathered}Y_1 \oplus Y_3 = X_1 \oplus X_3, Y_2 \oplus Y_4 = X_2 \oplus X_3 \\ X_5^{'}, X_6^{'} = MA(Y_1 \oplus Y_3, Y_2 \oplus Y_4) \\ \Rightarrow X_5^{'}, X_6^{'} = X_5, X_6\end{gathered}$$

$$Y_1^{'} = Y_1 \oplus X_5^{'} = X_1 \oplus X_5 \oplus X_5 = X_1$$

Similarly, $Y_2^{'} = X_2, Y_3^{'} = X_3, Y_4^{'} = X_4$

Finally

$$\begin{gathered}X_1, X_2, X_3, X_4 = In(Y_1, Y_2, Y_3, Y_4) \\ X_1, X_2, X_3, X_4 = In(In(X_1, X_2, X_3, X_4))\end{gathered}$$