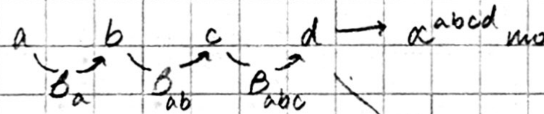
Aaron Hong
Prof. Poovendran
EE 418
11/27/23

1. a. h is preimage resistant because it is hard to find x given h(x) = y
this is because for most x values, finding the preimage requires solving the discrete logarithm problem
b. h is not collision resistant because since n is fixed for all x, there will be multiples of n for different x that result in the same y

2. a. $0.75 = \epsilon$, $Q = \sqrt{2M\ln(1/1-\epsilon)} = \sqrt{2(2^{256})\ln(4)} = \sqrt{2^{257}\ln(4)}$
$M = 2^{256}$ $= \sqrt{2^{258}\ln(2)} \approx 0.833 \cdot 2^{129}$
b. This hash function is second preimage resistant because it is collision resistant
c. This hash function is also collision resistant, making it second preimage resistant

3. $M = 12$, $Q = 4$, $\epsilon = 1 - e^{-4(4-1)/2(12)} = 1 - e^{-12/24} = 1 - 1/\sqrt{e} = 0.393$

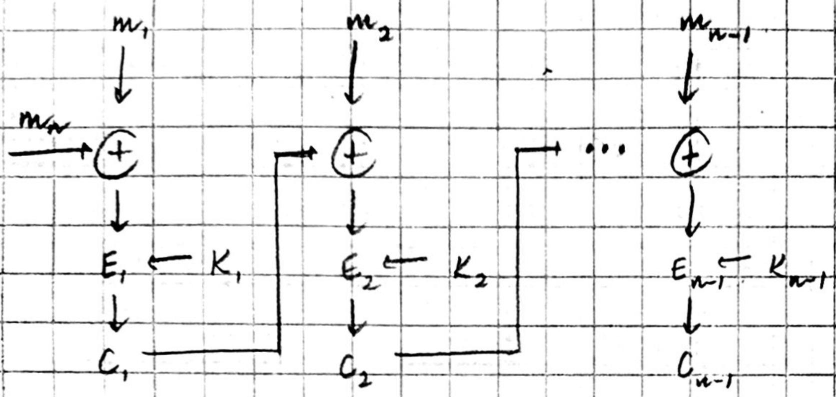
4. first, all 4 people calculate α^x where x is the person's prime. each person then transmits β_x to the next person over, and everyone calculates β_{xy}. This process repeats two more times until every person has received a β value 3 times. At the end of this process, everyone will end up with the same secret key $\alpha^{abcd} \bmod p$.



This process also starts from b, c, and d.

5. if h_1 is a collision resistant hash function, $h_1(x_1) \| h_2(x_2)$ is already collision resistant on its own. Putting the whole thing through h_1, it will remain collision resistant
By definition of collision resistance $h_1(x_1) = h_1(x_2)$ implies $x_1 = x_2$.

6.



b. for $m = 101011$ with key $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, block length 2

for original algorithm, $C_1 = 01$, $C_2 = 11$, $C_3 = 00$
for new algorithm, $C_1 = 10$, $C_2 = 00$, $C_3 = 00$
Therefore, the new algorithm gives a different result than the original