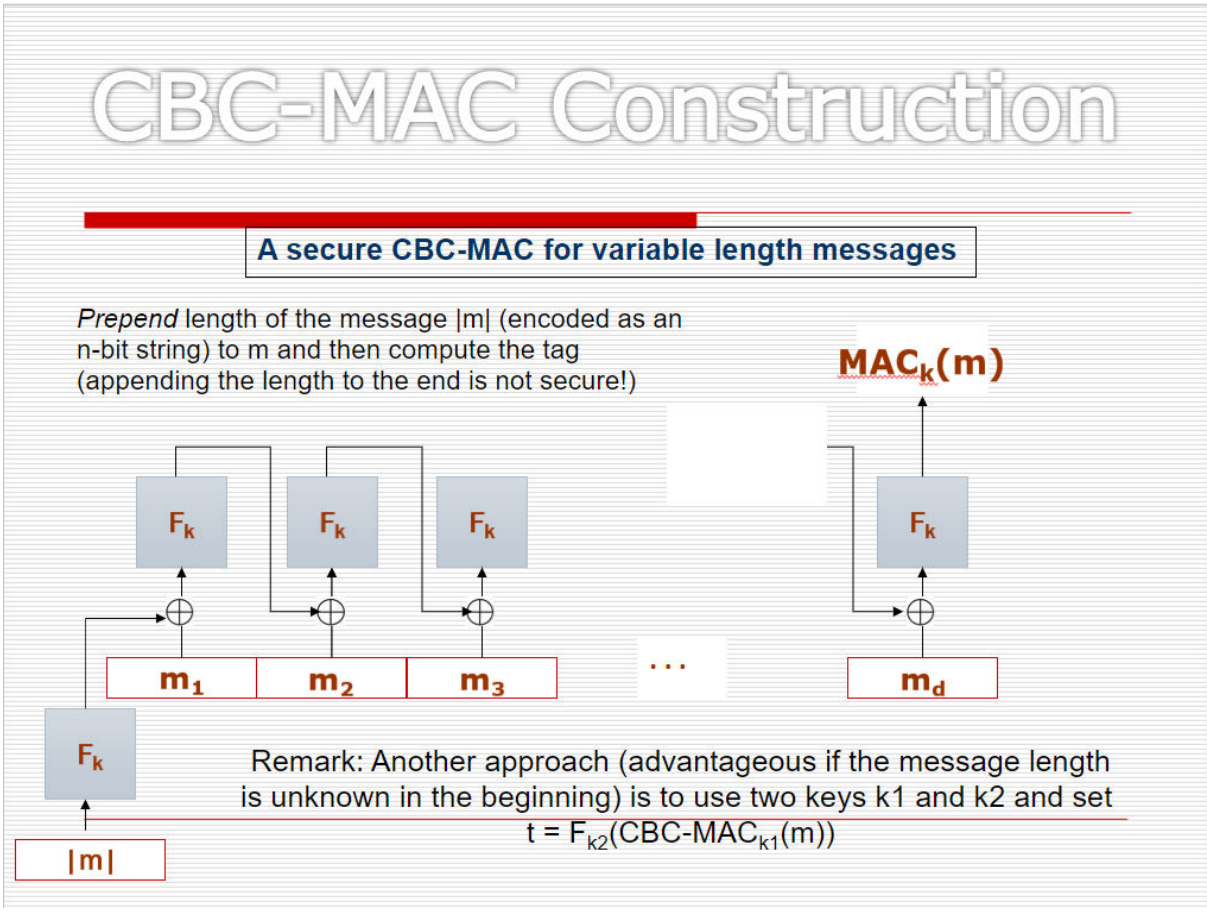
Sudipta Halder (2021202011)

Use the PRF to build a secure MAC

We will follow the below diagram for secure CBC-MAC construction for variable length messages.



[1]

Here, I've used previously built PRG and PRF to construct this CBC-MAC.

Working Flow:

1. First, we asked for input: prime(p), generator(g), key, data, block-size.
2. It will then check whether the data length is multiple of (block-size = key-size). If not, then it will pad zeros after the data to make the data length multiple of the key length.
3. Then, it will divide the data into blocks of block-size.
4. Then it will follow the CBC construction[1].
5. In first step, the binary encoded data length will passed through the PRF. The obtained prf result will be then xored with the first message block and passed through the PRF again.
6. For the next steps, the obtained prf from the previous iteration and the corresponsing msg block will be xored and then passed through PRF.

7. In this way, the last output from the PRF block will be used as MAC TAG.