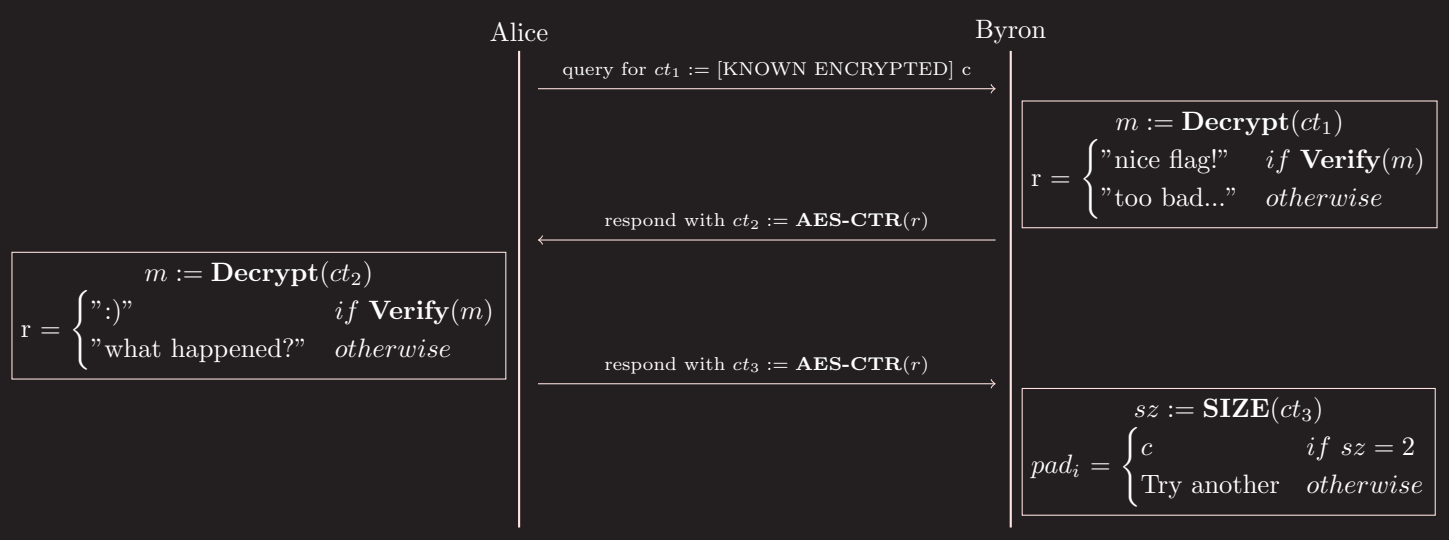
Alice
Byron
query for $ct_1$ := [KNOWN ENCRYPTED] c
$m := \mathbf{Decrypt}(ct_1)$
r = ”nice flag!” if $\mathbf{Verify}(m)$; ”too bad...” otherwise
respond with $ct_2 := \mathbf{AES\text{-}CTR}(r)$
$m := \mathbf{Decrypt}(ct_2)$
r = ”:)” if $\mathbf{Verify}(m)$; ”what happened?” otherwise
respond with $ct_3 := \mathbf{AES\text{-}CTR}(r)$
$sz := \mathbf{SIZE}(ct_3)$
$pad_i$ = $c$ if $sz = 2$; Try another otherwise