University of Maryland
CMSC414 — Computer and Network Security
Professor Jonathan Katz

Consider the following authentication protocol between two parties Alice and Bob who share a key k in advance. (Note: we did not yet cover authentication protocols in detail. For this problem, the level of security we are looking for is that an adversary should be unable to impersonate Alice to Bob, even after eavesdropping on multiple executions of the protocol between the two parties.)

1. Bob chooses a random value $r \in \{0,1\}^{128}$ and sends it to Alice.
2. Alice computes $c \leftarrow \mathsf{Enc}_k(r)$ and sends c to Bob.
3. Bob computes $r' = \mathsf{Dec}_k(c)$ and accepts if and only if $f' = r$.

Answer the following questions:

1. Show an encryption scheme that is secure against chosen-plaintext attacks, but would lead to an insecure protocol if plugged into the above.
2. Show an encryption scheme that is not secure against chosen-plaintext attacks, but would lead to a secure protocol if plugged into the above.
3. What is the "right" primitive to use in this setting? Suggest how to design a secure variant of the above protocol using this primitive.