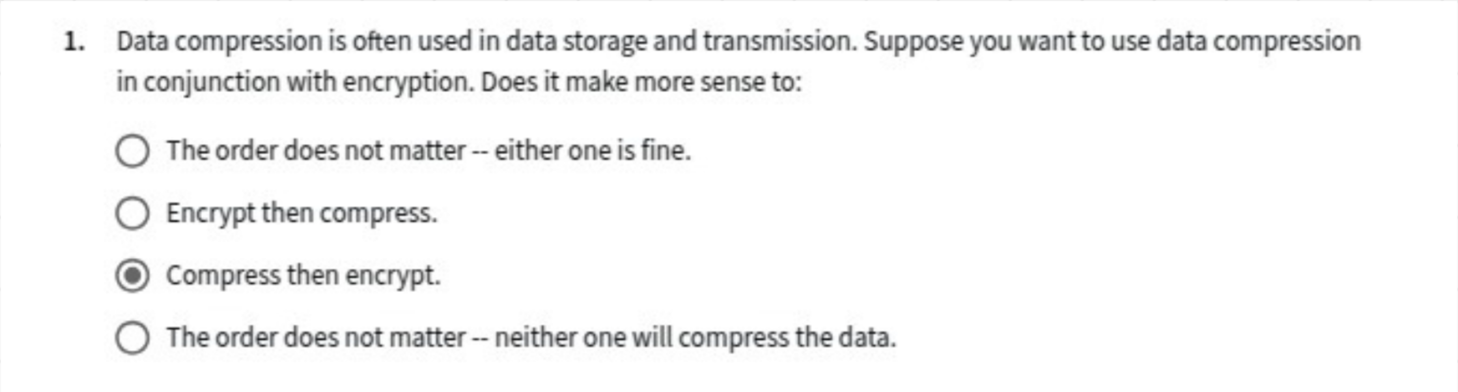
test #1



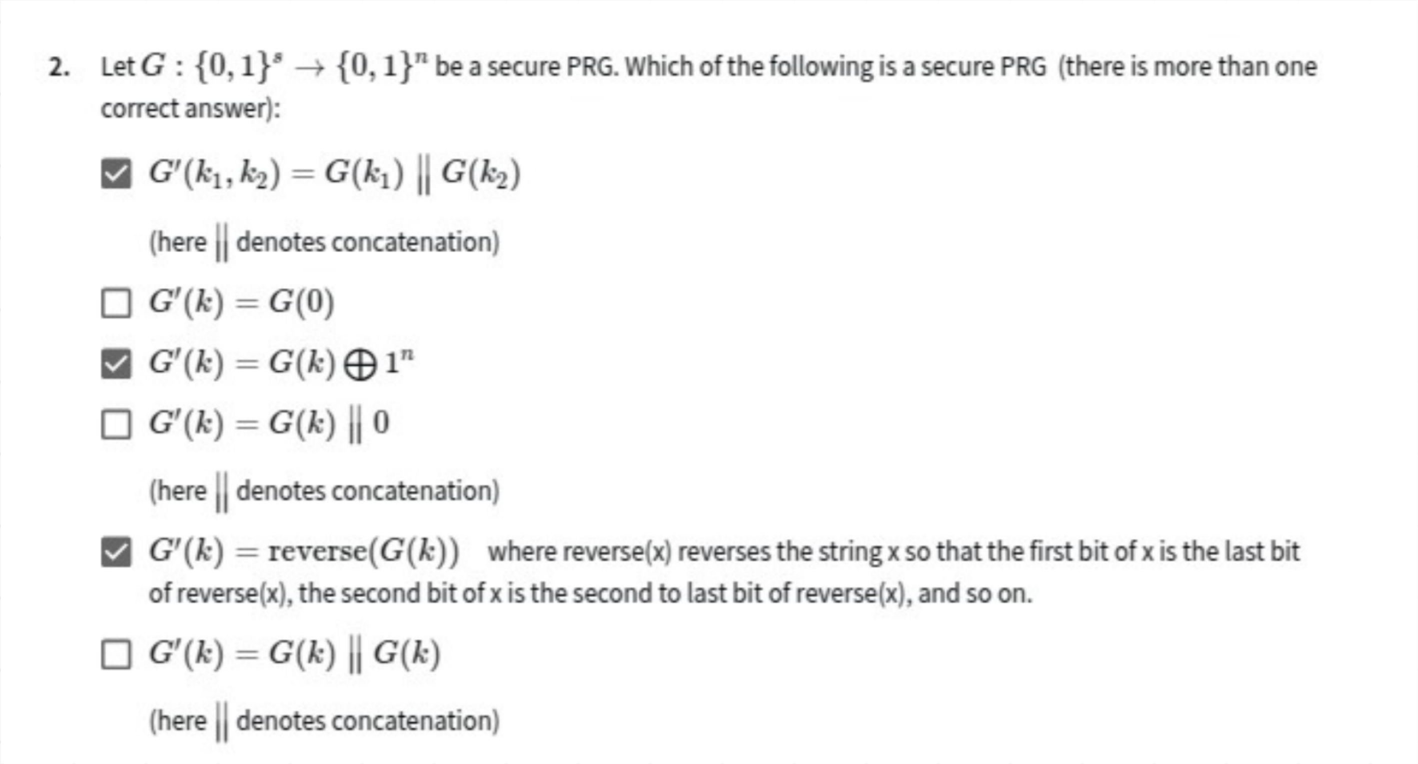
1. Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to:

○ The order does not matter -- either one is fine.

○ Encrypt then compress.

● Compress then encrypt.

○ The order does not matter -- neither one will compress the data.



2. Let $G : \{0,1\}^s \to \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG (there is more than one correct answer):

☑ $G'(k_1, k_2) = G(k_1) \parallel G(k_2)$

(here $\parallel$ denotes concatenation)

□ $G'(k) = G(0)$

☑ $G'(k) = G(k) \bigoplus 1^n$

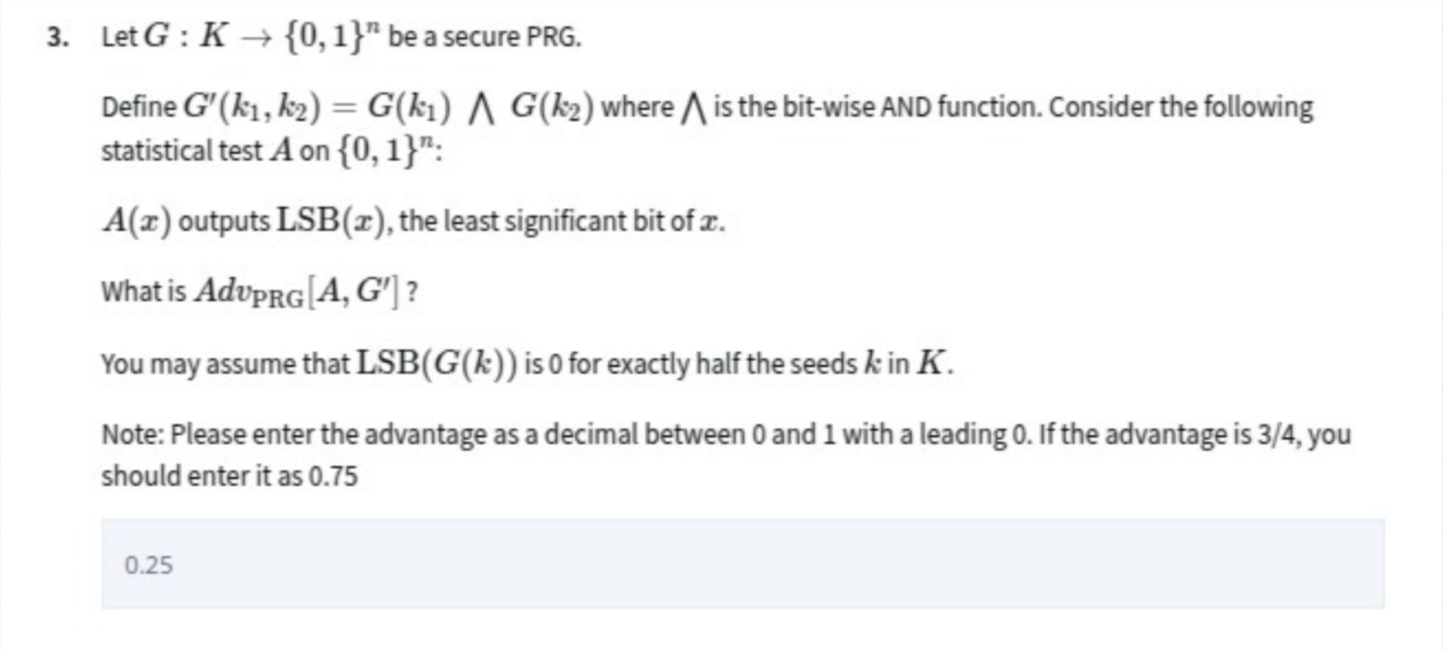
□ $G'(k) = G(k) \parallel 0$

(here $\parallel$ denotes concatenation)

☑ $G'(k) = \text{reverse}(G(k))$ where reverse(x) reverses the string x so that the first bit of x is the last bit of reverse(x), the second bit of x is the second to last bit of reverse(x), and so on.

□ $G'(k) = G(k) \parallel G(k)$

(here $\parallel$ denotes concatenation)



3. Let $G : K \to \{0,1\}^n$ be a secure PRG.

Define $G'(k_1, k_2) = G(k_1) \bigwedge G(k_2)$ where $\bigwedge$ is the bit-wise AND function. Consider the following statistical test A on $\{0,1\}^n$:

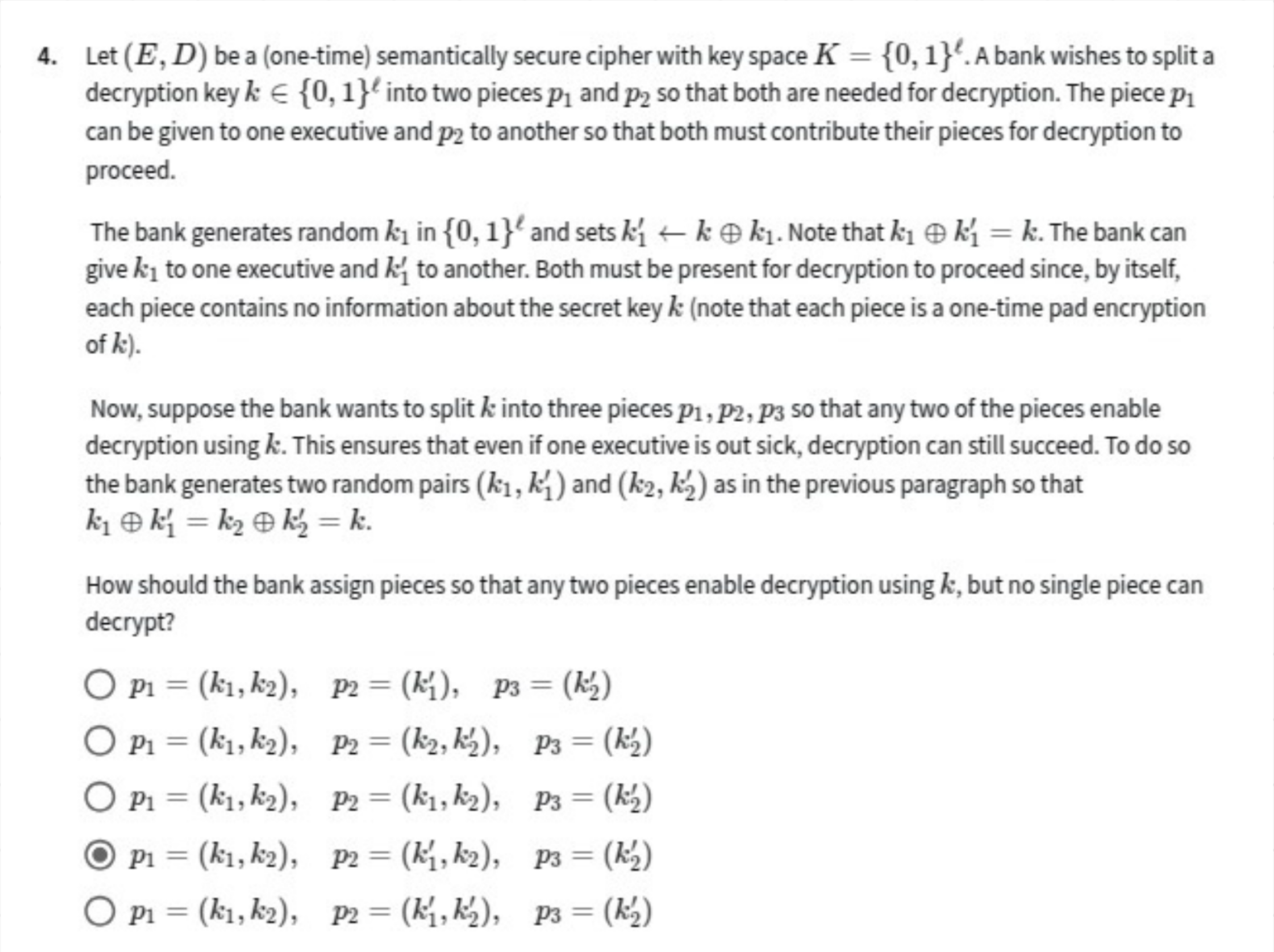
$A(x)$ outputs $\text{LSB}(x)$, the least significant bit of x.

What is $Adv_{\text{PRG}}[A, G']$?

You may assume that $\text{LSB}(G(k))$ is 0 for exactly half the seeds k in K.

Note: Please enter the advantage as a decimal between 0 and 1 with a leading 0. If the advantage is 3/4, you should enter it as 0.75

0.25



4. Let (E, D) be a (one-time) semantically secure cipher with key space $K = \{0,1\}^\ell$. A bank wishes to split a decryption key $k \in \{0,1\}^\ell$ into two pieces p_1 and p_2 so that both are needed for decryption. The piece p_1 can be given to one executive and p_2 to another so that both must contribute their pieces for decryption to proceed.

The bank generates random k_1 in $\{0,1\}^\ell$ and sets $k_1' \leftarrow k \oplus k_1$. Note that $k_1 \oplus k_1' = k$. The bank can give k_1 to one executive and k_1' to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k).

Now, suppose the bank wants to split k into three pieces p_1, p_2, p_3 so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decryption can still succeed. To do so the bank generates two random pairs (k_1, k_1') and (k_2, k_2') as in the previous paragraph so that $k_1 \oplus k_1' = k_2 \oplus k_2' = k$.

How should the bank assign pieces so that any two pieces enable decryption using k, but no single piece can decrypt?

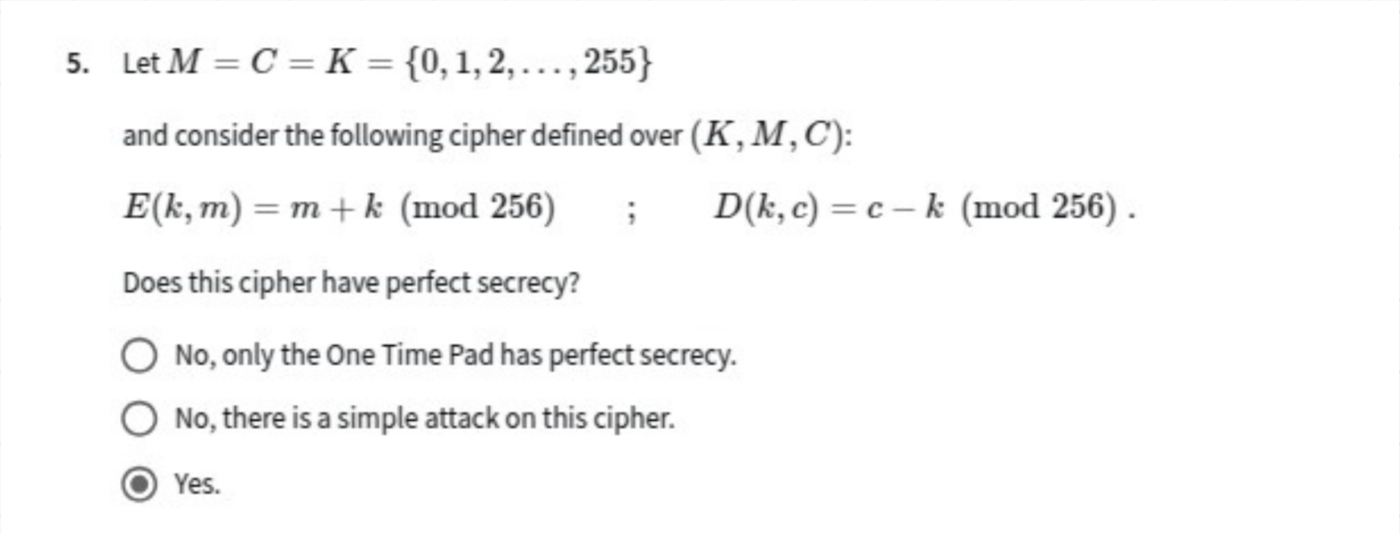
○ $p_1 = (k_1, k_2), \quad p_2 = (k_1'), \quad p_3 = (k_2')$

○ $p_1 = (k_1, k_2), \quad p_2 = (k_2, k_2'), \quad p_3 = (k_2')$

○ $p_1 = (k_1, k_2), \quad p_2 = (k_1, k_2), \quad p_3 = (k_2')$

● $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2), \quad p_3 = (k_2')$

○ $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2'), \quad p_3 = (k_2')$



5. Let $M = C = K = \{0, 1, 2, \ldots, 255\}$

and consider the following cipher defined over (K, M, C):

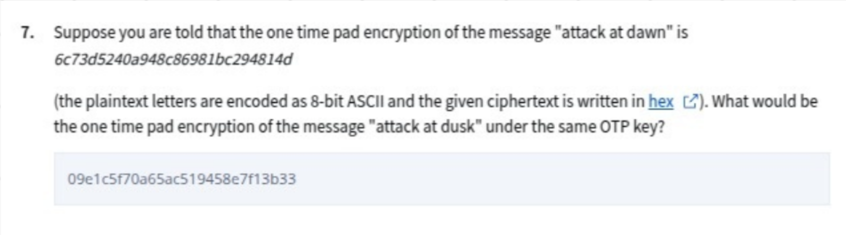
$$E(k, m) = m + k \pmod{256} \qquad ; \qquad D(k, c) = c - k \pmod{256} \,.$$

Does this cipher have perfect secrecy?

○ No, only the One Time Pad has perfect secrecy.

○ No, there is a simple attack on this cipher.

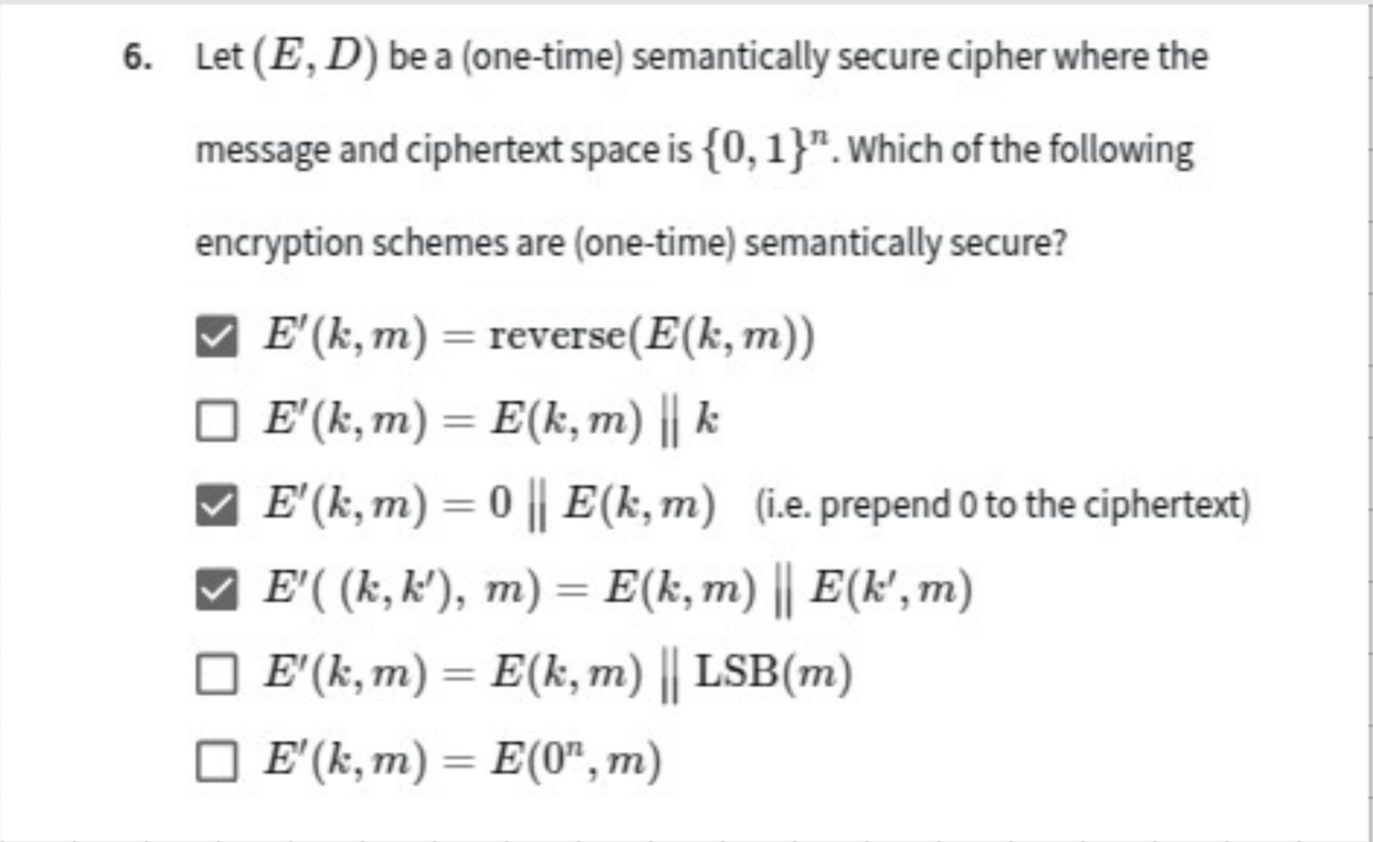
● Yes.



7. Suppose you are told that the one time pad encryption of the message "attack at dawn" is *6c73d5240a948c86981bc294814d*

(the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex ↗). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key?

09e1c5f70a65ac519458e7f13b33



6. Let (E, D) be a (one-time) semantically secure cipher where the message and ciphertext space is $\{0,1\}^n$. Which of the following encryption schemes are (one-time) semantically secure?

☑ $E'(k,m) = \text{reverse}(E(k,m))$

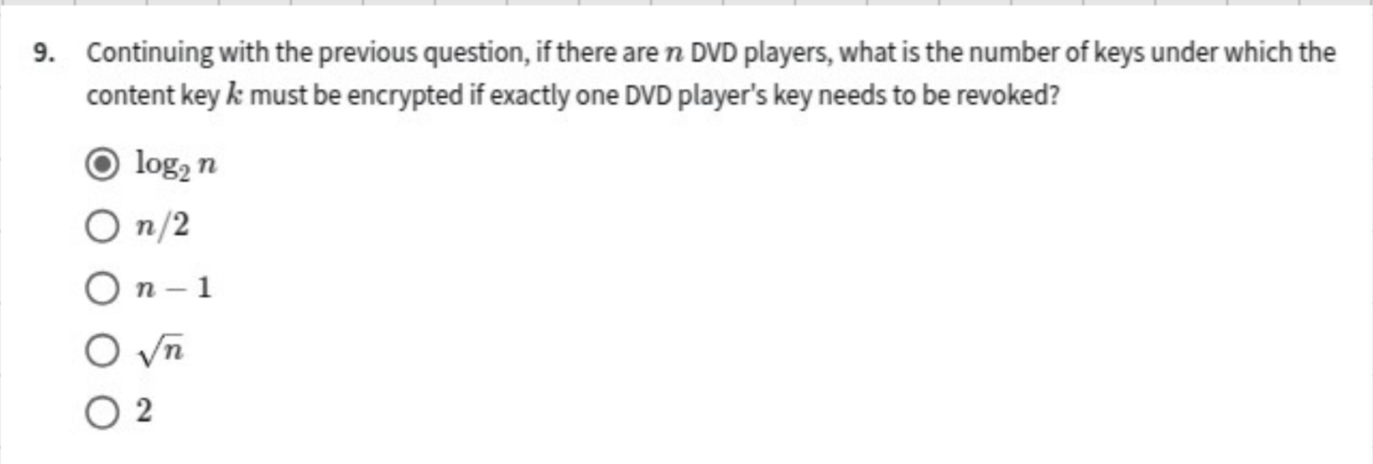
□ $E'(k,m) = E(k,m) \parallel k$

☑ $E'(k,m) = 0 \parallel E(k,m)$ (i.e. prepend 0 to the ciphertext)

☑ $E'(\ (k,k'),\ m) = E(k,m) \parallel E(k',m)$

□ $E'(k,m) = E(k,m) \parallel \text{LSB}(m)$

□ $E'(k,m) = E(0^n,m)$



9. Continuing with the previous question, if there are n DVD players, what is the number of keys under which the content key k must be encrypted if exactly one DVD player's key needs to be revoked?

● $\log_2 n$

○ $n/2$

○ $n-1$

○ $\sqrt{n}$

○ 2