Week #1 Extra

Notation:

Note: reverse denotes the function that takes a bit string and produces the reverse bit.

- || denotes the concatenation of strings.
- $\oplus$ denote the bit-wise XOR operation.
- x^n is the representation of n time x in the sequence, e.g. $0^3 = 000$.
- $\leftarrow \$$ denotes generating uniformly random values from a given set.

G_1

secure encryption scheme (E, D), with a message and ciphertext space $\{0,1\}^n$.

Alternative encryption scheme (E', D'), which will be built from (E, D)

G_1: which of the encryption schemes E' are correct ($\forall m, k. D'(k, E'(k, m)) = m$?

1. $E'(k,m) = reverse(E(k,m))$
   $D'(k,c) = reverse(D(k,c))$

   1) ciframos com E': $E'(k,m) = reverse(E(k,m))$
      - isso cifra m utilizando o esquema original E
      - Depois inverte a string de bits resultante

   2) Deciframos com D': $D'(k, E'(k,m)) = reverse(D(k, E'(k,m))$

$D'(k, \underbrace{reverse(E(k,m))}_{c}))$ $= reverse(D(k, \underbrace{reverse(E(k,m))}_{c}))$

R: Este esquema não é correto, pois $D'(k,E'(k,m)) \neq m$.

2.

$E'(k,m) = E(0^n, m)$

$D'(k,c) = (D(0^n, c))$

$D'(K, \underbrace{E(\underbrace{0^n}_{k}, \underbrace{m}_{m})}_{c}) = (D(0^n, E(0^n, m)))$

$D'(k, E'(k,m)) = D(0^n, E(0^n, m)) = m$ ✓

R: Este esquema é correto.

3. $E'(k,m) = E(k,m) \| 10$

$D'(k,c) = D(k, c[0 \ldots n])$

$D'(k,c) = D(k, c[0 \ldots n])$

$D'(k, E'(k,m)) = D(k, \underbrace{E(k,m)}_{c} \| 10 [0 \ldots n])$

$D'(k, E' k, m) = D(k, E(k,m) \| 10 [0 \ldots n]) = m$ ✓

R: Este esquema é correto.

4. $E'(k,m) = E(k,m) \oplus 1^m$

$D'(k,c) = D(k,(c \oplus 1^m))$

$D'(k, E'(k,m)) = D(k, (\underbrace{E(k,m) \oplus 1^m}_{c} \oplus 1^m)$

$= D(k, (E(k,m) \cancel{\oplus 0}$

$D'(k, E'(k,m) = D(k, (E(k,m))) = m$ ✓

5. $E'(k,m) = \underbrace{E(k, 0^n)}_{c}$

$D'(k,c) = D(k, 0^n)$

$D'(k, E'(k,m)) = D(k, 0^n)$

R: não é correto pois $D(k, 0^n)$ não tem c, então não conseguimos avançar.

6. $E'(k,m) = E(k,m) \,||\, m$

$D'(k,c) = D(k, c[0 \ldots n])$

$D'(k, E'(k,m)) = D(k, E(k,m) \,||\, m[0 \ldots n])$

$= D'(k, E'(k,m)) = m$ ✓