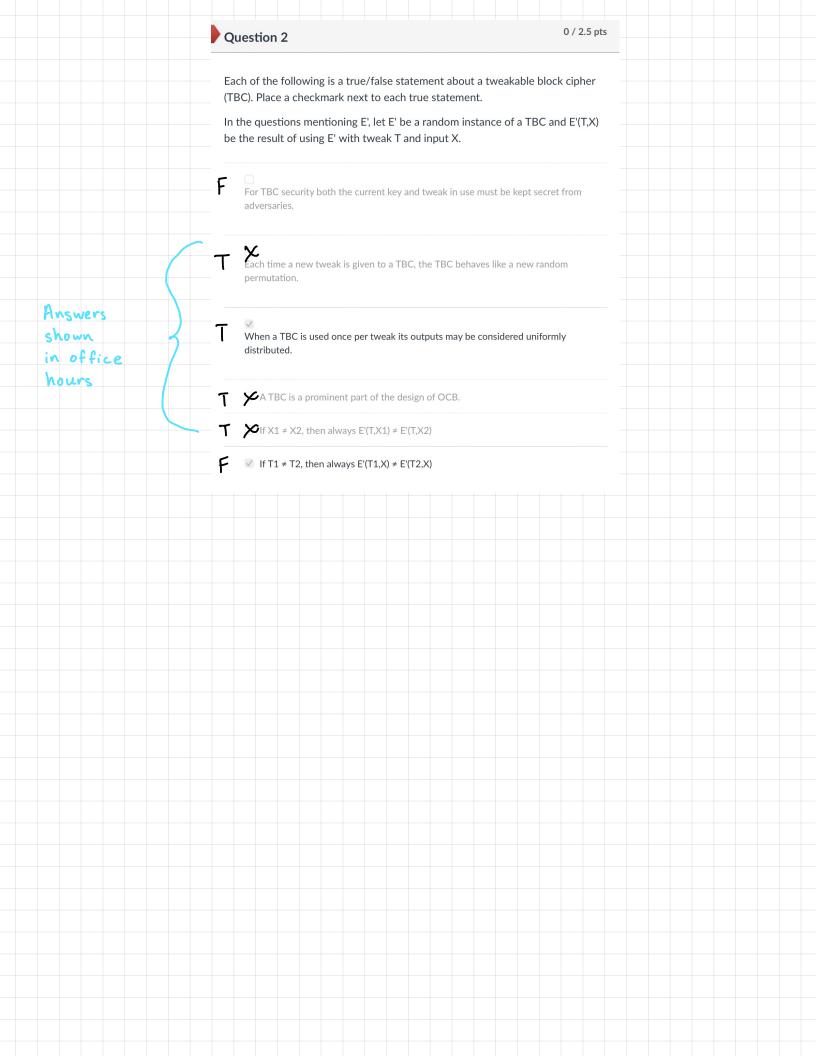
A trick die has eight sides that are equally likely to face up. The numbers on the eight sides are 1, 2, 3, 4, 1, 6, 7, 8. That's right, two sides are marked 1 and none are marked 5. How many bits of entropy are there with respect to what number faces up when the die is rolled? Round your answer to the nearest hundredth.

2.75

Outcomes	Pr	Entropy	Product
1	2 8	$-\log_2(\frac{2}{8}) = 2$	$\frac{2}{8} \cdot 2 = \frac{1}{2}$
2	18	$-\log_{2}(\frac{2}{8}) = 2$ $-\log_{2}(\frac{1}{8} = 3)$	$\frac{1}{8} \cdot 3 = \frac{3}{8}$
3	18	3	<u>3</u>
ч	1 8	3	3 8
6	18	3	3 8
7	18	3	3 8
8	18	3	8
			2.75



I showed you in lecture how OCB uses a tweakable block cipher (TBC). It uses the universal hash function  $h(T) = (iv)2^{T}$  where each message has its own random iv and calculation is over a Galois field. The TBC is then constructed as E'(T,X) = h(T) xor E(X xor h(T)). This hash function is optimized for finding h(T+1)

For this problem we'll use  $GF(2^8)$  whose modulus is  $x^8 + x^4 + x^3 + x + 1$ . If h(0) is 11001101 (in binary or CD in hex), what are h(1) and h(2)?

h(1) 81

h(2) 19

Answer each with exactly 8 binary digits or 2 hex digits, and no spaces.

$$iv = x^7 + x^6 + x^3 + x^2 + 1$$

$$h(1) = (iv) 2 = (CD) 2 = 19A$$

$$X(x^{7}+x^{6}+x^{3}+x^{2}+1) = x^{8}+x^{7}+x^{4}+x^{3}+x$$

$$h(2) = (iv) 2^2 = (CD) 4 = 334 (Hex)$$

$$x^{2}(x^{7}+x^{6}+x^{3}+x^{2}+1) = x^{9}+x^{8}+x^{5}+x^{4}+x^{2}$$

$$x^{4} + x^{3} + 1$$

