Question 1

2.5 / 2.5 pts

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	$\frac{2}{8}$	$-\log_2(\frac{2}{8}) = 2$	$\frac{2}{8} \cdot 2 = \frac{1}{2}$
2	$\frac{1}{8}$	$-\log_2(\frac{1}{8} = 3$	$\frac{1}{8} \cdot 3 = \frac{3}{8}$
3	$\frac{1}{8}$	3	$\frac{3}{8}$
4	$\frac{1}{8}$	3	$\frac{3}{8}$
6	$\frac{1}{8}$	3	$\frac{3}{8}$
7	$\frac{1}{8}$	3	$\frac{3}{8}$
8	$\frac{1}{8}$	3	$\frac{3}{8}$
			2.75

Question 2

0 / 2.5 pts

Each of the following is a true/false statement about a tweakable block cipher (TBC). Place a checkmark next to each true statement.

In the questions mentioning E', let E' be a random instance of a TBC and E'(T,X) be the result of using E' with tweak T and input X.

F ☐ For TBC security both the current key and tweak in use must be kept secret from adversaries.

T ☒ Each time a new tweak is given to a TBC, the TBC behaves like a new random permutation.

T ☑ When a TBC is used once per tweak its outputs may be considered uniformly distributed.

T ☒ A TBC is a prominent part of the design of OCB.

T ☒ If X1 ≠ X2, then always E'(T,X1) ≠ E'(T,X2)

F ☑ If T1 ≠ T2, then always E'(T1,X) ≠ E'(T2,X)

Answers shown in office hours

Question 3

2.5 / 2.5 pts

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) given h(T).

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.

$h(T) = (iv)\,2^T$

$h(0) = 1100\ 1101 = CD\ (Hex)$

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

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

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

$x^8 + x^4 + x^3 + x + 1 \;\overline{)\; x^8 + x^7 + x^4 + x^3 + x}$

1

$x^8 + x^4 + x^3 + x + 1$

$81\ (Hex) \qquad x^7 + 1$

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

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

$x^8 + x^4 + x^3 + x + 1 \;\overline{)\; x^9 + x^8 + x^5 + x^4 + x^2}$

x

$x^9 + x^5 + x^4 + x^2 + x$

$x^8 + x$

$x^8 + x^4 + x^3 + x + 1 \;\overline{)\; x^8 + x}$

1

$x^8 + x^4 + x^3 + x + 1$

$x^4 + x^3 + 1$

$19\ (Hex)$

Question 4

2.5 / 2.5 pts

Let's now say that we are using as our block cipher the S-box from AES (ie, imagine that we have given a block cipher a key and it has given us the AES S-box as our permutation to use).

If h(0) = 11001101 (in binary or CD in hex), then using the construction and hash function from the previous problem, what are the following values?

E'(1, 00000000) 8D

E'(2, 10101010) 74

Answer each with exactly 8 binary digits or 2 hex digits, and no spaces. You can find the AES S-box on Page 101 of https://www.crypto-textbook.com/download/Understanding-Cryptography-Chapter4.pdf

$$E'(T, x) = h(t) \text{ xor } E(x \text{ xor } h(T))$$

Table 4.3 AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

$$h(1) \text{ xor } E(00000000 \text{ xor } h(1))$$

$$= 81 \oplus E(0 \oplus 81)$$

$$= 81 \oplus S(81)$$

$$= 81 \oplus 0C$$

$$= 8D$$

$$h(2) \text{ xor } E(10101010 \text{ xor } h(2))$$

$$= 19 \oplus E(AA \oplus 19)$$

$$= 19 \oplus S(B3)$$

$$= 19 \oplus 6D$$

$$= 74$$