Question 1

2 / 2 pts

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

F ☐ Because of its extra features, a TBC is always much slower than a regular block cipher.

F ☐ A good TBC allows change of the key with little computational cost.

T ☑ A good TBC allows change of the tweak with little computational cost.

F ☐ A tweakable block cipher is a prominent part of the design of GCM.

F ☐ Each time a new tweak is given to a TBC, the TBC behaves like a new random function.

T ☑ Each time a new tweak is given to a TBC, the next output of the TBC is uniformly distributed.

Question 2

2 / 2 pts

Each of the following is a true/false statement about authenticated encryption. Place a checkmark next to each true statement.

F ☐ The only benefit to authenticated encryption is the ability to use the same key for both authentication and encryption.

F ☐ OCB is the most used authenticated encryption algorithm.

T ☑ OCB is faster than GCM.

F ☐ GCM is essentially a univeral-hash-based authentication paired with CBC-mode encryption.

F ☐ Patents slowed the adoption of GCM.

F ☐ GCM completes encryption before it begins authentication.

Question 3

2 / 2 pts

How many bits of entropy are there in the result of throwing a pair of four-sided dice (each side numbered 1, 2, 3, 4) and summing the two resulting values?

Answer to the nearest thousandth.

2.65

Outcome	Pr	Entropy if all equal	Product
2	$\frac{1}{16}$	$-\log_2(\frac{1}{16}) = 4$	$\frac{1}{16} \cdot 4 = \frac{1}{4}$
3	$\frac{2}{16}$	$-\log_2(\frac{2}{16}) = 3$	$\frac{2}{16} \cdot 3 = \frac{3}{8}$
4	$\frac{3}{16}$	$-\log_2(\frac{3}{16}) = 2.42$	$\frac{3}{16} \cdot 2.42 = 0.45$
5	$\frac{4}{16}$	$-\log_2(\frac{4}{16}) = 2$	$\frac{4}{16} \cdot 2 = \frac{1}{2}$
6	$\frac{3}{16}$	$-\log_2(\frac{3}{16}) = 2.42$	$\frac{3}{16} \cdot 2.42 = 0.45$
7	$\frac{2}{16}$	$-\log_2(\frac{2}{16}) = 3$	$\frac{2}{16} \cdot 3 = \frac{3}{8}$
8	$\frac{1}{16}$	$-\log_2(\frac{1}{16}) = 4$	$\frac{1}{16} \cdot 4 = \frac{1}{4}$

Sum = 2.65

2 = (1,1)

3 = (1,2), (2,1)

4 = (1,3), (3,1), (2,2)

5 = (1,4), (4,1), (2,3), (3,2)

6 = (2,4), (4,2), (3,3)

7 = (3,4), (4,3)

8 = (4,4)

Total # of outcomes possible = 16

Question 4

2 / 2 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 demonstration purposes let's do an example over $GF(2^8)$. If h(0) is 42 (in hex), what are h(1) and h(2)?

h(1) 84

h(2) 13

Answer each with a two-digit hex answer and no spaces.

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

$h(0) = 42$ (hex)

$h(0) = 0100\ 0010$

$h(0) = x^6 + x$

$h(0) = iv$

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

$h(1) = (iv)\,2 = 66 \times 2 = 132 \Rightarrow 84$ (hex)

$84 = 1000\ 0100 = x^7 + x^2$

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^7 + x^2$ — quotient: 0

$h(1) = x^7 + x^2 = 84$

$h(2) = x^5 + x^2 + x = 26$ (hex)

$h(2) = 66 \times 2^2 = 264 = 108$ (hex)

$= 0001\ 0000\ 1000$

$= x^8 + x^3$

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^8 + x^3$ — quotient: 1

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

$x^4 + x + 1$

$x^4 + x + 1 = 13$

Question 5

2 / 2 pts

Let's now say that we are using as our blockcipher 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) = 42, then using the construction and hash function from the previous problem, what are the following values?

E'(1, 00000000) DB

E'(2, 10101010) 45

Answer each with a two-digit hex answer and no spaces.

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

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

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

$$= 84 \oplus E(0 \oplus 84)$$

$$= 84 \oplus S(84)$$

$$= 84 \oplus 5F$$

$$= DB$$

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

$$= 13 \oplus E(AA \oplus 13)$$

$$= 13 \oplus S(B9)$$

$$= 13 \oplus 56$$

$$= 45$$