All additions are modulo 2 unless specified otherwise.

Practice Exam 1

1. Alice and Bob share a 3-bit random key. Alice encrypts 3-bit message $m = m_1m_2m_3$ to ciphertext $c = (m_1 + k_2k_3, m_2 + k_3k_1, m_3 + k_1k_2)$.

   (a) The shared key is $k = \texttt{011}$. Bob receives $c = \texttt{010}$. What does Bob decrypt to?

   Solution: To decrypt, Bob adds the ciphertext to $(k_2k_3, k_3k_1, k_1k_2) = \texttt{100}$. The message is $\texttt{110}$.

   (b) Eve observes ciphertext $c = \texttt{010}$. Is it more likely that Alice's message is $\texttt{010}$ or $\texttt{011}$?

   Solution: If $m = \texttt{010}$, the required mask is $c + m = \texttt{000}$. This mask is produced by the four keys of Hamming weight at most one: $\texttt{000}, \texttt{001}, \texttt{010}, \texttt{100}$. If $m = \texttt{011}$, the required mask is $\texttt{001}$, which is produced only by $k = \texttt{110}$. Thus $\texttt{010}$ is four times as likely as $\texttt{011}$.

2. Alice's and Bob's shared key is a random permutation P of the English alphabet. Alice encrypts message $m = xyz\ldots$ as

$$P(x), P(P(x) + y), P(P(P(x) + y) + z), \ldots$$

   Additions here are modulo 26.

   (a) What does FWL decrypt to under the following shared key?

	0				5				10				15				20				25				
x:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
P(x):	M	C	I	X	U	O	R	T	G	W	Z	E	B	V	P	Y	Q	J	F	S	A	N	L	D	H	K

   Solution: The message symbols are

$$x = P^{-1}(\texttt{F}) \qquad y = P^{-1}(\texttt{W}) - \texttt{f} \qquad z = P^{-1}(\texttt{L}) - \texttt{w}.$$

   Plugging in

$$P^{-1}(\texttt{F}) = 18, \qquad P^{-1}(\texttt{L}) = 9, \qquad P^{-1}(\texttt{L}) = 22,$$

   we obtain $x = 18, y = 9 - 5 = 4, z = 22 - 22 = 0$. The message is $\boxed{\texttt{sea}}$.

   (b) Alice encrypts 100 consecutive as. What is the probability that the ciphertext consists of the same symbol repeated 100 times?

   Solution: The encryption of m_1 has the form $P(0), P(P(0)), P(P(P(0)))$, and so on. The first and second symbol repeat if and only if $P(0) = 0$. Moreover, if they do, all the other symbols are also the same. As there are 26 equally likely choices for $P(0)$, this is an event of probability $1/26$.

   (c) Now Alice encrypts a sequence of 100 uniformly random letters. What is the probability that the ciphertext consists of the same symbol repeated 100 times?

   Solution: When P is fixed, the cipher has the same input and output length. When instantiated on a uniformly random input, its output will also be uniformly random. The probability that it consists of the same symbol repeated 100 times is $26 \cdot 26^{-100} = 26^{-99}$.

3. F is a pseudorandom function with 32 bits of input and output. Its key is shared between Alice and Bob. To encrypt a 64-bit message, Alice splits it into left and right halves m_L and m_R, chooses random 16-bit pointers x and y and sends $(x, y, m_L + F(x, y), m_R + F(y, x))$ to Bob.

(a) How should Bob decrypt?

Solution: On input (x, y, c_L, c_R), Bob computes

$$m_L = c_L + F(x, y), \qquad m_R = m_R + F(y, x).$$

In words, he evaluates F on (x, y) and (y, x) and adds the results with the two masked halves.

(b) Assume Eve's advantage in distinguishing F from a random function is about 2^{-32}. Her advantage in distinguishing an encryption from a sequence of truly random bits is

about 2^{-32} | **about 2^{-16}** | about $1/2$

Solution: With probability 2^{-16}, $x = y$. Then the two calls to F are identical, so the two 32-bit pads are equal. For truly random output bits, two independent 32-bit pads are equal with probability only 2^{-32}. This collision test gives advantage about 2^{-16}, which dominates the stated 2^{-32} PRF advantage.

If F were truly random, on the other hand, then conditioned on $x \neq y$, the output is sampled exactly like a random string with distinct x and y. The distinguisher has no advantage substantially higher than 2^{-16}.

(c) Now Eve observes another encryption. Eve's new distinguishing advantage is

about the same as in (b) | **about twice as large as in (b)** | close to 1

Solution: Either encryption can have $x = y$. The probability of at least one such event is

$$1 - (1 - 2^{-16})^2 \approx 2 \cdot 2^{-16}.$$

Collisions between inputs belonging to different encryptions have probability only on the order of 2^{-32} and do not change this estimate.

Practice Exam 2

1. Alice's and Bob's secret key is a random permutation P on 3 bit strings. To encrypt a 9-bit message, Alice applies P on each 3-bit block.

   (a) P is given by the table below. What does 001011111 encrypt to? What does 111110000 decrypt to?

x	000	001	010	011	100	101	110	111
$P(x)$	101	011	100	111	110	001	000	010

   Solution: Encryption is blockwise:

$$001011111 \longmapsto P(001)P(011)P(111) = 011111010.$$

   For decryption, $P^{-1}(111) = 011$, $P^{-1}(110) = 100$, and $P^{-1}(000) = 110$. Hence

$$111110000 \longmapsto 011100110.$$

   (b) Among which pairs of the following messages can Eve distinguish their encryptions?

$$m_1 = 000000001 \qquad m_2 = 001001000 \qquad m_3 = 000001000$$

   Solution: Equality of plaintext blocks is preserved by a permutation. In m_1 and m_2, the first two blocks are equal and the third is different. In m_3, the first and third blocks are equal. Therefore Eve can distinguish m_1 from m_3, and m_2 from m_3. She cannot distinguish m_1 from m_2 by this pattern. Both ciphertexts consist of two random equal 3-bit sequences followed by a random different 3-bit sequence.

2. Let y_0 to y_6 be the first seven bits output by the following cipher:

State: A 5-bit register $s = s_4s_3s_2s_1s_0$.
Init: Set s to equal the 5-bit key k.
Next: Set *next* to $s_2 + s_0$ mod 2.
Output $s_0 + s_1s_2$.
Right shift all other bits of s.
Set the leftmost bit of s to *next*.

   (a) Calculate y_0 to y_6 when $k = 00000$ and when $k = 11111$.

   Solution: For $k = 00000$ the state remains zero, so

$$y_0 \cdots y_6 = 0000000.$$

   For $k = 11111$, the successive states are

$$11111, 01111, 00111, 00011, 10001, 11000, 11100,$$

   which give

$$y_0 \cdots y_6 = 0001100.$$

   (b) Each of the bits y_0 to y_6 is indistinguishable from a pure random bit. **true** **false**

   Solution: True. The values of the state bits in terms of the key are

$$s_0 = k_0, \cdots, s_4 = k_4, s_5 = k_0 + k_2, s_6 = k_1 + k_3, s_7 = k_2 + k_4, s_8 = k_0 + k_2 + k_3.$$

   Each y_i equals $k_{i \bmod 5}$ plus some function that is independent of it. It is therefore indistinguishable from a pure random bit.

(c) All parities $y_i + y_j + y_k$ of 3 distinct bits are indistinguishable from a pure random bit. **true** **false**

Solution: False. As $s_5 = s_0 + s_2$,

$$y_0+y_2+y_5 = s_0+s_1s_2+s_2+s_3s_4+s_5+s_6s_7 = s_1s_2+s_3s_4+s_6s_7 = k_1k_2+k_3k_4+(k_1+k_3)(k_2+k_4) = k_1k_4+k_2k_3.$$

The bits k_1k_4 and k_2k_3 are indepdendent. Each is equal to 1 with probability 1/4. There sum is equal to one when one is 1 and the other is 0, or with probability $2 \cdot 1/4 \cdot 3/4 = 3/8$.

3. P is a pseudorandom permutation on 4 bits. Its key is shared between Alice and Bob. To encrypt a 8-bit message m, Alice splits it into a left half m_L and a right half m_R, chooses a random pad x, and sends

$$(x, P(x + m_L), P(x + m_R + \texttt{1111})).$$

(a) Bob receives ciphertext (x, c_L, c_R). How should Bob decrypt it?

Solution: Bob computes

$$m_L = x + P^{-1}(c_L), \qquad m_R = x + P^{-1}(c_R) + \texttt{1111}.$$

(b) Let $m_1 = \texttt{00000000}, m_2 = \texttt{00000101}, m_3 = \texttt{00111100}$. Circle all pairs of messages whose encryptions Eve can distinguish. Describe the distinguisher.

m_1 and m_2 $\qquad$ $\boxed{m_1 \text{ and } m_3}$ $\qquad$ $\boxed{m_2 \text{ and } m_3}$

Solution: The two PRP inputs are equal exactly when

$$x + m_L = x + m_R + \texttt{1111},$$

or equivalently $m_L = m_R + \texttt{1111}$. This holds for $m_3 = \texttt{0011 1100}$ but not for m_1 or m_2.

Encryptions of m_1 and m_2 are therefore insdistinguishable. They consist of a random pad x follows by two random distinct values.

Encryptions of m_1 and m_3 can be distinguished by D that accepts when $c_L \neq c_R$. This is always true for encryptions of m_1 and never true for encryptions of m_2. As encryptions of m_1 and m_2 are perfectly indistinguishable, the same D tells apart encryptions of m_2 from those of m_3.

(c) Eve observes encryptions $c_3 = (\texttt{0000}, \texttt{0011}, \texttt{1111})$, $c_4 = (\texttt{0000}, \texttt{1111}, \texttt{0000})$ of messages m_3 and m_4. Circle the only possibility for m_3 and m_4 among the following alternatives:

$$\texttt{00000000} \qquad \texttt{00001111} \qquad \texttt{01011111} \qquad \texttt{11110000}.$$

Solution: Since the pointer x is zero in both instantiations and P is a permutation, it must be that

$$m_{3L} \neq m_{3R} + \texttt{1111} \qquad m_{4L} = m_{3R} + \texttt{1111} \qquad m_{4L} \neq m_{4R} + \texttt{1111}.$$

The first and last condition rule out $\texttt{00001111}$ and $\texttt{11110000}$. The remaining condition is satisfied for

$$\boxed{m_3 = \texttt{01011111}, \qquad m_4 = \texttt{00000000}}.$$

Practice Exam 3

1. G is the following sampler that takes in 5 pure random bits and produces 6 output bits:

$$G(k_1k_2k_3k_4k_5) = (k_1 + k_4, k_1 + k_5, k_2 + k_4, k_2 + k_5, k_3 + k_4, k_3 + k_5).$$

Alice encrypts message m under shared key k as $m + G(k)$. Let

$$m_1 = \texttt{000000} \qquad m_2 = \texttt{000001} \qquad m_3 = \texttt{111111}.$$

(a) Eve can distinguish an encryption of m_1 from an encryption of m_2. **true** **false**

Solution: True. Every output $z = G(k)$ satisfies

$$z_1 + z_2 + z_3 + z_4 = 0,$$

so this parity is always 0 for an encryption of m_1. Flipping the last bit, as in an encryption of m_2, does not affect this particular parity; instead use

$$z_1 + z_2 + z_5 + z_6 = 0.$$

For m_2, this parity is always 1.

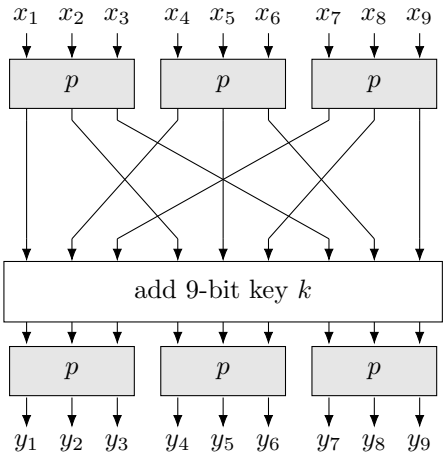
(b) Eve can distinguish an encryption of m_1 from an encryption of m_3. **true** **false**

Solution: False. If $\overline{k} = k + \texttt{11100}$, then $G(\overline{k}) = G(k) + \texttt{111111}$. Since $\overline{k}$ is uniform whenever k is uniform, $G(k)$ and $G(\overline{k}) = G(k) + m_3$ have the same p.m.f.

(c) Eve can distinguish an encryption of m_1 followed by an encryption of m_2 (under the same key) from an encryption of m_3 followed by an encryption of m_2. **true** **false**

Solution: True. Eve adds the two ciphertexts. In the first case the result is $m_1 + m_2 = \texttt{000001}$; in the second it is $m_3 + m_2 = \texttt{111110}$.

2. This question concerns the following substitution-permutation network P.



x	000	001	010	011	100	101	110	111
$p(x)$	101	011	100	111	110	001	000	010

(a) Calculate $P(\texttt{000000000})$ and $P^{-1}(\texttt{000000000})$ when $k = \texttt{101010101}$.

Solution: For the forward direction,

$$\texttt{000000000} \xrightarrow{p} \texttt{101101101} \xrightarrow{\text{perm}} \texttt{111000111} \xrightarrow{+k} \texttt{010010010} \xrightarrow{p} \boxed{\texttt{100100100}}.$$

Reversing the operations gives

$$\texttt{000000000} \xrightarrow{p^{-1}} \texttt{110110110} \xrightarrow{+k} \texttt{011100011} \xrightarrow{\text{perm}^{-1}} \texttt{010110101} \xrightarrow{p^{-1}} \boxed{\texttt{111000000}}.$$

(b) What is the probability that $P(\texttt{000000000}) = \texttt{111111111}$?

Solution: As the 9-bit key is purely random, the value entering the last layer of p-boxes is uniform. Since the last layer is a permutation, the output is uniform. Therefore the probability is $2^{-9} = 1/512$.

(c) Eve observes that $P(\texttt{000000000}) = \texttt{111111111}$. What can she deduce about $P^{-1}(\texttt{000000000})$?

Solution: The observation determines the key. Before the last p-layer the state must be

$$p^{-1}(\texttt{111})^3 = \texttt{011011011}.$$

The fixed state before key addition on input zero is $\texttt{111000111}$, so

$$k = \texttt{111000111} + \texttt{011011011} = \texttt{100011100}.$$

Decrypting zero under this key gives

$$\boxed{P^{-1}(\texttt{000000000}) = \texttt{111000111}}.$$

3. R is a random permutation on 3 bit strings. R' is the function

$$R'(xy) = (R(x), R(y) + k)$$

where k is a 3-bit random key (independent of R), and x, y are 3-bit strings.

(a) R' is a permutation on 6-bit strings for every k. (**Hint:** Is it invertible?) **true** **false**

Solution: True. Given $(u, v) = R'(x, y)$, recover

$$x = R^{-1}(u), \qquad y = R^{-1}(v + k).$$

(b) For every input xy, $R'(xy)$ is indistinguishable from a truly random 6-bit string. **true** **false**

Solution: True. The first half $R(x)$ is uniform. Independently, the uniform key k makes the second half $R(y) + k$ uniform and independent of the first, even when $x = y$.

(c) For every pair of distinct inputs $xy \neq x'y'$, the output pair $(R'(xy), R'(x'y'))$ is indistinguishable from a pair of distinct truly random 6-bit strings. **true** **false**

Solution: False. Take two distinct inputs with $x = x'$ and $y \neq y'$, e.g. $xy = \texttt{000000}$ and $x'y' = \texttt{000111}$. The distinguisher accepts if their first output halves are equal. This is always true for $(R'(xy), R'(x'y'))$, but quite unlikely for two random distinct strings. Once the first string is fixed, there are exactly 2^3 out of $2^6 - 1$ choices that make the first 3 bits of the second string match. The probability the distinguisher accepts this pair is $2^3/(2^6 - 1) = 8/63$.