

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 $k = 011$. Bob receives $c = 010$. What does Bob decrypt to?
- (b) Eve observes ciphertext $c = 010$. Is it more likely that Alice's message is 010 or 011?

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

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

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				

- (b) Alice encrypts 100 consecutive as. What is the probability that the ciphertext consists of the same symbol repeated 100 times?
 - (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?
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?
- (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 $1/2$

- (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

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

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

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

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 $s_2 + s_0 \bmod 2$.

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 $k = 11111$.

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

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

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

$$(x, P(x + m_L), P(x + m_R + 1111)).$$

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

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

$$m_1 \text{ and } m_2 \quad m_1 \text{ and } m_3 \quad m_2 \text{ and } m_3$$

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

$$00000000 \quad 00001111 \quad 01011111 \quad 11110000.$$

Practice Exam 3

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

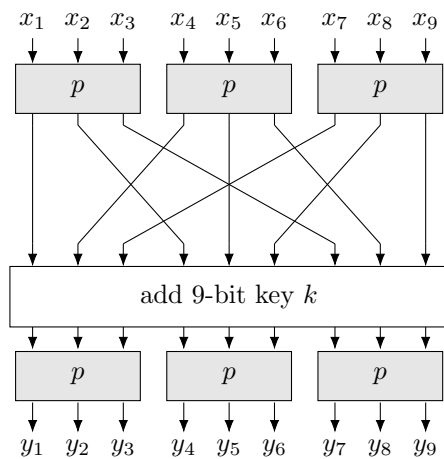
$$G(k_1 k_2 k_3 k_4 k_5) = (k_1 + k_4, k_1 + k_5, k_2 + k_4, k_2 + k_5, k_3 + k_4, k_3 + k_5).$$

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

$$m_1 = 000000 \quad m_2 = 000001 \quad m_3 = 111111.$$

- (a) Eve can distinguish an encryption of m_1 from an encryption of m_2 . **true** **false**
- (b) Eve can distinguish an encryption of m_1 from an encryption of m_3 . **true** **false**
- (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**

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 $P(000000000)$ and $P^{-1}(000000000)$ when $k = 101010101$.
- (b) What is the probability that $P(000000000) = 111111111$?
- (c) Eve observes that $P(000000000) = 111111111$. What can she deduce about $P^{-1}(000000000)$?

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