1 Don't Reuse that One-Time Pad

Here are five 4-letter (upperase) messages in ASCII each XORed using the same key $k \in \{0,1\}^{32}$. Recover all the messages and then encrypt the word MATH using the same key:

- $E(k, m_1) =$ 10011111 01110001 01100001 11001101
- $E(k, m_2) =$ 10001110 01100010 01110111 11001011
- $E(k, m_3) =$ 10000000 01110001 01101011 11001010
- $E(k, m_4) =$ 10001110 01100010 01110111 11010111
- $E(k, m_5) =$ 10000110 01110001 01110111 11001101

Here's a table of ASCII values for the uppercase letters:

A	65	01000001		N	78	01001110
B	66	01000010		O	79	01001111
C	67	01000011		P	80	01010000
D	68	01000100		Q	81	01010001
E	69	01000101		R	82	01010010
F	70	01000110		S	83	01010011
G	71	01000111		T	84	01010100
H	72	01001000		U	85	01010101
I	73	01001001		V	86	01010110
J	74	01001010		W	87	01010111
K	75	01001011		X	88	01011000
L	76	01001100		Y	89	01011001
M	77	01001101		Z	90	01011010

Proof. [SOLUTION: Hint: E is the most common letter of the alphabet.
Key k: 11001011 00110100 00110010 10011001
Words: TEST, EVER, KEYS, EVEN, MEET

$$E(k, \text{“}MATH''\text{)} = \texttt{10000110 01110101 01100110 11010001}$$

] $\square$

2 One-Time Pad Overkill

2.1

Suppose we use a double-key for OTP:

$$\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2 = \{0,1\}^n \times \{0,1\}^n$$
$$\mathcal{M} = \{0,1\}^n$$
$$\mathcal{C} = \{0,1\}^n$$

- $E((k_1, k_2), m) = k_1 \oplus k_2 \oplus m$
- $D((k_1, k_2), c) = k_1 \oplus k_2 \oplus c$

Prove that this cipher has perfect secrecy. (Make sure to use the definition of perfect secrecy.)

Proof. [SOLUTION: For any $m \in \mathcal{M}, c \in \mathcal{C}$:

$$Pr[E(k \xleftarrow{R} \mathcal{K}, m) = c] = \frac{2^n}{2^n \cdot 2^n}$$

Thus, the definition of perfect secrecy holds if we compare any two messages.] □

2.2

Do the same for:

- $\mathcal{K} = \{0,1\}^n \times \{0,1\}$
- $E((k_1, b), m) = k_1 \oplus \underbrace{bb...b}_{n} \oplus m$

(The bit string $\underbrace{bb...b}_{n}$ is n copies of b.)

Proof. [SOLUTION: For any $m \in \mathcal{M}, c \in \mathcal{C}$:

$$Pr[E(k \xleftarrow{R} \mathcal{K}, m) = c] = \frac{2}{2^n \cdot 2}$$

] □

3 Caesar Cipher's Shaky Secrecy (Say *that* ten times.)

Consider the Caesar Cipher:

$$\mathcal{M} = \mathcal{C} = \{0, ..., 25\}^n$$
$$\mathcal{K} = \{0, ..., 25\}$$

- $E(k, m) = \Big[(m[0] + k \bmod 26), ..., (m[n-1] + k \bmod 26)\Big]$
- $D(k, c) = \Big[(c[0] - k \bmod 26), ..., (c[n-1] + k \bmod 26)\Big]$

Prove that it does not have perfect secrecy.
Proof. [SOLUTION: Consider $m_0 = [0, 0]$ and $m_1 = [0, 1]$ and $c = [0, 0]$ Now:

$$Pr[E(k \xleftarrow{R} \mathcal{K}, m_0) = c] = 1/26$$
$$Pr[E(k \xleftarrow{R} \mathcal{K}, m) = c] = 0$$

Thus, the Caesar Cipher does not have perfect secrecy.] $\square$

4 Analyze that Cipher!$^{\text{TM}}$

Suppose we have a cipher

- $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
- $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

that has perfect secrecy. Consider the following ciphers that are built on it. Which ones have perfect secrecy? Prove/disprove it.

4.1

- $\mathcal{K}' = \mathcal{K}$
- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{C}' = \mathcal{C} \times \{0,1\}^8$
- $E'(k,m) := (E(k,m), \texttt{01101100})$
- $D'(k,(c_1,c_2)) = D(k,c_1)$

Proof. [SOLUTION: Consider $c \in \mathcal{C}$. Then:

$$\begin{aligned} Pr[E(k,m) = c] &= Pr[(E(k,m), \texttt{01101100}) = (\texttt{c}, \texttt{01101100})] \\ &= Pr[E'(k,m) = (c, \texttt{01101100})] \end{aligned}$$

Thus, we have perfect secrecy.
] □

4.2

- $\mathcal{K}' = \mathcal{K}$
- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{C}' = \mathcal{C} \times \mathcal{K}$
- $E'(k,m) = (E(k,m), k)$
- $D'(k,(c_1,c_2) = D(k,c_1)$

Proof. [SOLUTION: This does not have perfect secrecy.

Consider an encryption $c = (c_1, c_2) = E(k \xleftarrow{R} \mathcal{K}, m)$ of a message m. This means that $k = c_2$.

Suppose another message m' can encrypt to the same ciphertext. Since

$$E(k', m') = c = (c_1, c_2)$$

this means that $k' = c_2 = k$.

However, we also know that $D(k,c) = m$. Thus, two messages cannot encrypt to the same ciphertext, and we definitely don't have perfect secrecy.
] □

4.3

- $\mathcal{K}' = \mathcal{K} \times \mathcal{K}$
- $\mathcal{M}' = \mathcal{M}$
- $\mathcal{C}' = \mathcal{C} \times \mathcal{K}$
- $E'((k_1, k_2), m) = (E(k_2 \oplus k_1, m), k_1)$
- $D'((k_1, k_2), (c_1, c_2)) = D(k_2 \oplus k_1, c_1)$

5 Bonus binary boolean function of the day: NOR

5.1

Consider the NOR binary function

a	b	$NOR(a, b)$
0	0	1
0	1	0
1	0	0
1	1	0

Show how to write $a \oplus b$ using only (nested) NOR functions with a and b.

Proof. [SOLUTION:

$$NOR(NOR(a, b), NOR(NOR(a, a), NOR(b, b)))$$

] □

5.2

Try the same for $NAND$:

a	b	$NAND(a,b)$
0	0	1
0	1	1
1	0	1
1	1	0

Proof. [SOLUTION:

$$NAND(NAND(a, NAND(a,b)), NAND(b, NAND(a,b)))$$

] □

6 More RSA

Suppose someone knows $\varphi(N)$ for a public RSA modulus N. Show how they can factor N without additional information.

Proof. [SOLUTION:

- $N = p \cdot q$
- $\varphi(N) = (p-1) \cdot (q-1)$
- $N = 1 - \varphi(N) = p + q$

We know $p \cdot q$ and $p + q$, so we can solve for p and q using standard quadratic techniques:

$$p = \frac{1}{2}\left(-\sqrt{(\mathrm{N} - \varphi(N) + 1)^2 - 4\mathrm{N}} + \mathrm{N} - \varphi(N) + 1\right)$$
$$q = \frac{1}{2}\left(\sqrt{(\mathrm{N} - \varphi(N) + 1)^2 - 4\mathrm{N}} + \mathrm{N} - \varphi(N) + 1\right)$$

] □

7 More ElGamal Encryption

Suppose Eve listens in on an ElGamal encryption from Alice to Bob. That is, she sees Bob publishing

$$(p, g, h = g^x)$$

and sees Alice sending

$$(c_1 = g^y, c_2 = m \cdot h^y)$$

Show that if Eve can find out m without any additional information, she has broken an instance of the Computational Diffie-Hellman Problem (show the exact givens for the problem instance, and how she finds the secret value in the CDH Problem).

Proof. [SOLUTION: Suppose Alice has m.

The instance is

$$(g, g^x, g^y)$$

and Eve finds

$$g^{xy}$$

by calculating

$$c_2 \cdot m^{-1} (\bmod\ p) = h^y = g^{xy}$$

] $\square$