The method we employed to decipher this text is essentially a brute force search of every possible combination of 8-bit numbers, from 00000000 to 11111111. As integers, this ranges from 0 – 255, and thus we were able to simply search within a range of 0 to 256.

The algorithm our code utilizes uses python’s ergonomic method of splitting text up by size and storing it in a structured list. Thus, after reading in the cipher text, we simply split it by 8-bit increments to represent each char size. The actual algorithm was very simple as well.

For each possible key from 0 – 256, we went through each 8-bit character, converted it to an integer and xored with the key, then converted it back to a char and appended it to the deciphered list of characters. Then, after outputting, it is easy to see if this is deciphered or not. This method will produce 256 different deciphered texts; only one is the correctly deciphered texts, using the correct key.

As stated, this is an extremely flimsy “one-time pad key”. Given the information that it was xored with the same key for each character, brute forcing this is extremely fast. Never-the-less, brute forcing through all possible options does not give us an efficient way of breaking a cypher-text. If a more thought out approach was taken, brute forcing could be maximized to take upwards of trillions, to 2^100000, to negligible amounts of attempts before even coming close to breaking the code. Even then, we would either have to have humans scanning the text the entire time to assess when the code has actually been broken, or implement some sort of logic scanner that would actually notify the system when it has assessed the code has been broken based on relative human speech formatting of word patterns. Obviously there aren’t even enough people on the planet to justify the first approach to brute-forcing a decoded message, and either way these would illustrate just how expensive brute forcing would be. For this reason it is very safe to assume that we are the adversary, and we are very aware of the context, because otherwise, we would be in a very tight spot attempting to brute force attack this text.

Other alternatives to brute forcing an entire key space to find meaning in plaintext would involve attacks such as statistical attacks, known-plaintext attacks, or chosen plain or cipher text attacks. A statistical attack involves knowing some statistical information about, say, the sender of the cipher text, and being able to use that information as a starting point in the brute force method, or to skip entire portions of possibilities altogether. The other options all involve some sort of pre-knowledge about the attack as well; such as common names that can be found in the cypher-text, and thus giving clues as to how to go about decrypting it.

As illustrated, it is extremely difficult to brute-force attack a cipher-text unless given some sort of background information. Given the information that it is encoded using a one-time 8-bit pad (which is also conveniently the size of a char in most languages), it becomes quite easy comparably to brute-force attack this text by narrowing down the possibilities greatly. Thus, we are left with the decrypted text:

Call me Ishmael. Some years ago--never mind how long precisely--having little or no money in

my purse, and nothing particular to interest me on shore, I thought I would sail about a little and

see the watery part of the world. It is a way I have of driving off the spleen and regulating the

circulation. Whenever I find myself growing grim about the mouth; whenever it is a damp, drizzly

November in my soul; whenever I find myself involuntarily pausing before coffin warehouses,

and bringing up the rear of every funeral I meet; and especially whenever my hypos get such an

upper hand of me, that it requires a strong moral principle to prevent me from deliberately

stepping into the street, and methodically knocking people's hats off--then, I account it high time

to get to sea as soon as I can. This is my substitute for pistol and ball. With a philosophical

flourish Cato throws himself upon his sword; I quietly take to the ship. There is nothing

surprising in this. If they but knew it, almost all men in their degree, some time or other, cherish

very nearly the same feelings towards the ocean with me.