XOR Crypto

Using the programming language of your choice (so long as it is either compilable or interpretable on my Linux OS), implement the XOR crypto method. **Each team will submit one program**.

The method takes a message, m (either plaintext or ciphertext), of size b bytes and a key, k, also of size b bytes (i.e., they are exactly the same size). Each bit of m is XOR'd with each bit of k, one bit at a time. In practice, we use a buffer of some size (e.g., $4,096$ bytes or 4KB) and XOR a group of bits together for better performance.

Requirements:

- Submit your source code only (I will provide my own key and plaintext/ciphertext to test with);
- Read the key from a file named *key* in the current directory (make sure that this works on Linux; i.e., don't use Windows-specific directory separators);
- Read the plaintext/ciphertext from `stdin`; and
- Send generated output (either plaintext or ciphertext) to `stdout`.

Please, no GUIs. Make this a command line application without frills that I can execute as follows: `./xor < plaintext > ciphertext`. This would take the contents of *plaintext*, XOR (encrypt) it with the contents of *key*, and store the resulting ciphertext to *ciphertext*. The reverse: `./xor < ciphertext` would take the contents of *ciphertext*, XOR (decrypt) it with the contents of *key*, and send the resulting plaintext to `stdout`.