

Pre- and Post- Processing for Cryptography

Dr. Ostheimer, CS 14, Fall 2023

As the sender, before we encrypt, we need a way to convert our text to decimals that are suitable for encryption. We will call this process *pre-processing*. Likewise, when we receive a list of decimals representing an encrypted message, after we perform the decryption to get a new list of decimals, we need a way to convert this list to text. We will call this process *post-processing*. Here I will summarize one technique for pre- and post-processing.

Choose a B . We choose a positive integer B . How we choose it will depend on the crypto-system we are using.

Pre-processing: We start with text and we compute a list of decimals as follows.

1. Convert the text to a list of decimal numbers using ASCII.
2. Convert the list of decimal numbers to a list of 8-bit binary strings using binary notation.
3. Convert the list of 8-bit binary strings to one long binary string using concatenation.
4. Convert the long binary string to a list of B -bit binary strings by breaking up from the right and padding on the left with 0's as needed.
5. Convert the list of B -bit binary strings to a list of decimals using binary notation.

Post-processing: We start with a list of decimals, and we compute text as follows.

1. Convert the list of decimals to a list of B bit binary strings using binary notation.
2. Convert the list of B -bit binary strings to one long binary string using concatenation.
3. Convert the long binary string into a list of 8-bit binary strings by breaking up from the right and padding on the left with 0's as needed.
4. Convert the list of 8-bit binary strings to a list of decimals using binary notation. If you have a leading 0 as the first entry in this list of decimals, ignore it. (It comes from the padding that happened during encryption.)
5. Convert the list of decimals to text using ASCII.