OOP Project 1: AES

Szymon Wilczyński

What is AES

- AES (Advanced Encryption Standard) is a symmetric-key encryption standard that has been adopted by US government in 2002.
- It can use a key that has either 128, 192 or 256 bits.
- The plaintext is split into 128-bit chunks that are individually put through a series of rounds that produce ciphertext.

What problems I've encountered

- Time.
- Bitshifts casting the result to int.
- Couldn't fully understand some of the math involved.
- Something breaks at the string encoding phase, which spoils the result.

What I've learned

- Java.
- AES.

What could be improved

- Some of the calculations were replaced with lookup tables. Effective solution, but feels inelegant.
- Text to encrypt/decrypt could be loaded from a file instead of being passed as command line argument.