CS4600

Cryptography and Information Security

AES Algorithm Pseudocode

```
AES128Encrypt(){
    // filepath passed in on the command line
    src_filepath = get_commandline_parameter()

    // destination is filepath as the source with a ".enc" filename extension
    dst_filepath = get_dst_filepah(src_filepath)

    // 16 bytes taken from the user as hex digits with nothing echoed in the terminal
    key = get_key_from_user_input()

    key_schedule[11] = get_key_schedule(key)     // precalc all round-keys

    src_file_descriptor = open_file(src_filepath, read)  //open the plaintext file
    dst_file_descriptor = open_file(dst_filepath, write) //open the new ciphertext

    buffer[16] f_buffer  // a buffer of 16 bytes

    while src_file_descriptor != EOF do
        bytes_read = read_file(src_file_descriptor, f_buffer)

        // need 16 bytes of plaintext for each round.
        if bytes_read < 16 then pad_with_zero(f_buffer, bytes_read)

        key_add(key_schedule[0], f_buffer())  // pre-round key addition

        for i = 1 to 9 do
            sub_bytes(f_buffer)   // byte-substitution layer (use sbox map)
            shift_rows(f_buffer)  // shiftrow layer
            mix_columns(f_buffer) // shiftcol layer
            key_add(key_schedule[i], f_buffer()) // round-key addition
        next

        sub_bytes(f_buffer)
        shift_rows(f_buffer)
        key_add(key_schedule[10], f_buffer())

        // write 16 bytes of buffer to ciphertext file
        read_file(dst_file_descriptor, f_buffer, 16)
    loop

    close_file(src_file_descriptor)
    close_file(dst_file_descriptor)
}
```