CPS713 - LAB 3 - WRITTEN PORTION OF TASK 3

By: Francis, Matt; Huq, Reaz

1. I would not consider this cryptographic cipher to be secure. For one thing, the key size is a menial 2^9. Thus, to attack the ECB implementation, an attacker would only need to compute 512 keys and try each of them until they are able to decrypt the cipher-text and return a legible plaintext (in the case of attacking an encrypted picture, successfully cracking the key would result in a discernible image; in the case of attacking an encrypted sound file, successfully cracking the key would result in discernible sound.). Though rotating the key may serve a useful purpose in that it it appears reduces the viability of statistical attacks (as it diffuses the plaintext within the ciphertext for a given number of rounds), it may not be sufficiently large to dissuade an attacker from mounting a brute-force attack. Furthermore, the encryption algorithm does not adequately provide diffusion, since if it did, the output would be sufficiently randomized. The one-time run test and the birthday spacing tests (both found in the package **dieharder,** the successor to the diehard package. The one-time run test is also found in the NIST test suite) were both designed to test the efficacy of a random-number generator. If the lightweight-DES algorithm designed provided adequate diffusion, its output would exhibit pseudorandomness. This was not found to be the case, however, as subjecting the output of each of the ECB, CTR, and CBC algorithms (which encrypted a 500-word body of plain-English) resulted in output that did not pass either the birthday spacings test or the one-time run test. Unlike DES, which uses blocks of 64 bits, the algorithm developed takes blocks of 16 bits. A larger block size is desirable because it increases the possible mapping of each block of plaintext to a block of ciphertext.
2. The CBC encryption scheme is stronger than the ECB encryption scheme because the plaintext input is XOR'd with the ciphertext produced by the previous input of plaintext. Because it is assumed that the ciphertext is at least somewhat diffused, the plaintext is XOR'd with something that exhibits a degree of pseudorandomness. In the ECB mode of encryption, a block that is encrypted by the encryption function will always have the same output in the ciphertext when the same key is used.. Lastly due to the present block's ciphertext being dependant on previous blocks in CBC, the avalanche effect helps to add confusion to the encryption algorithm, as every change in a block makes the successive blocks of ciphertext harder to predict. One big problem with ECB is that the same sequence in plaintext will always look the same in the ciphertext [Stallings, 214]. This problem is addressed in CBC by the fact that the plaintext itself gets scrambled by an XOR with ciphertext before it enters the encryption function, which ensures that the plaintext will not be recognized the same way in each block. Of course, this advantage of CBC over ECB is negated if the message is smaller than the size of the block produced by the compression function.
3. The one-time pad is considered to be the strongest form of cryptography because its ideal implementation involves the use of a randomly generated key at each iteration. However strong the CBC mode of encryption is, because each iteration is produced from a block of plaintext, it may not exhibit complete diffusion (as there could be statistical

regularities inherent in the plain-text). The CTR mode of encryption exhibits an improvement in this regard as each block is XOR'd with something that is randomly generated independently of the plaintext. Likewise the CTR mode is not dependant on previous blocks, meaning that it is easily parallelizable, with multiple blocks undergoing encryption concurrently [Stallings, 223]. This allows the CTR mode of encryption to be significantly faster than CBC if implemented properly. Furthermore, the CTR mode of encryption is pre-processing friendly. It also allows for random access [Stallings, 224].

References

Text encrypted: https://pastebin.com/XtQjKUA3
https://webhome.phy.duke.edu/~rgb/General/dieharder.php Dieharder
STALLINGS, W. (n.d.). *CRYPTOGRAPHY AND NETWORK SECURITY: principles and practice, global edition*. UPPER SADDLE RIVER: PEARSON.