YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467: Cryptography and Computer Security *Handout #5*
Professor M. J. Fischer *September 21, 2020*

Homework Assignment 4

Due on Tuesday, September 29, 2020

1 Goal

The goal of this problem is to understand, explore, and analyze the security of a new cryptosystem.

2 SnakeOil

Our friend, Happy Hacker, has ignored my advice and decided to build his own cryptosystem, which he calls *SnakeOil*. He started with the botan implementation of AES-128 in CBC mode, but he decided to add his own padding and key management routines.

Padding Botan AES-128/CBC defaults to using PKCS#7 byte padding.[1] However, Happy was afraid that the redundancy it adds might make the code easier to crack since most incorrect keys will give a "decoding error" rather than a plausible-looking decryption. Instead, Happy decided to simply pad out the last incomplete block with zeros. For decoding, any trailing zero bytes in the last block are simply discarded. This works fine for text files, since they generally do not contain the zero (NUL) byte anyway, and it eliminates the possibility of decoding error exceptions.

Key Management Happy didn't think 128-bit keys were long enough, so he came up with a clever scheme for extending the key space. He first generates a file of 100 random 128-bit strings called *key shares*. He then computes a 128-bit *master key* to be used with AES. The master key is specified by two indices $0 \leq \texttt{idx1} < \texttt{idx2} < 100$. The *master key* is simply the exclusive-or of the two key shares with indices `idx1` and `idx2`, respectively.

Happy was pleased with his scheme and told his friends about all of its features.

1. It has a 12,800 bit key, which makes it far safer than AES's measly 128-bit key.

2. Happy reasons that it is now safe for him to store the key shares file on his hard disk since the file does not contain the master key and in fact is nothing more than a file of random numbers.

3. The only thing that Happy and his communication partners have to remember is the pair of key indices, both of which are numbers between 0 and 99. This is no more difficult than remembering the PIN for your bank ATM card.

[1] PKCS#7 padding is described on wikipedia page on "Padding (cryptography)".

3 Assignment

Answer the following questions concerning the usability and security of SnakeOil. Your answers should reflect what you have learned so far in the course about security in general and what it means for a cryptosystem to be secure.

1. What is good and bad about Happy's decision to replace PKCS#7 byte padding by zero-fill padding? Do you believe Happy's claim that it makes the code harder to crack? Why or why not?
2. Evaluate Happy's claim #1. What does Happy think the key is?
3. What is the effective key length of SnakeOil? To answer this question, you will need to be more specific than Happy was about what the actual key is.
4. Evaluate Happy's claim #2. Consider how different assumptions you can make about the security of the computer used to store the key shares file may affect your answer. What are the advantages of Happy's key management scheme?
5. Evaluate Happy's claim #3. How might an attacker exploit this feature that only the pair of key indices needs to be remembered?
6. Is SnakeOil secure under the conditions stated in Kerckhoffs's principle[2]? Why or why not?

[2] See the wikipedia page Kerckhoffs's principle.