Computer Security   Homework 3 (Due Friday 9/4/20)

1. 192-bit security is

   (a) trivial to break

   (b) pretty safe except against well-funded adversaries

   (c) somewhat safe now but likely won't be in another 5 years of typical technological gains

   (d) out of the reach of brute force for the foreseeable future

2. Suppose you capture some traffic encrypted with ordinary DES. If you want to decrypt it without having the key, which of the following is true?

   (a) There is no hope currently to brute-force the key.

   (b) You should make some friends in high places because only nation-states have the power to brute-force the key.

   (c) You should tag-team with 1000 of your closest friends. It will take you all a few years of continuous laptop computing time to finally brute-force the key.

   (d) Buy a nice GPU and set it to work for a few weeks to brute-force the key.

3. Repeat the question above but with DES replaced with triple DES.

4. Repeat the question above but with DES replaced with AES.

5. Which of the following is true about the development of AES?

   (a) AES is the name given to the cipher that was the winner of a worldwide contest in the late 1990s.

   (b) AES was designed by NIST and is only licensed to a few vendors worldwide.

   (c) AES is a continuously changing standard overseen by the National Security Agency. It evolved piece-by-piece from the older Data Encyrption Standard.

6. People believe AES is secure for which of the following reasons?

   (a) The algorithm's internals are closely guarded by NIST and are not publicly available.

   (b) The algorithm has been seriously scrutinized by professional cryptographers for over 20 years and no practical attacks have been found

7. What is wrong with using a block size of 64 bits in modern cryptography?

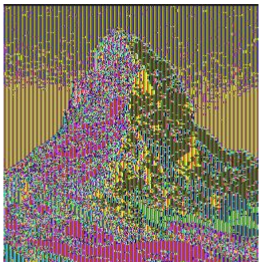
   (a) It is too slow.

   (b) People can easily build a table of size 2^{64} to perform a code book attack on the cipher.

   (c) It is subject to a birthday attack.

   (d) All of the above.

8. I found this encrypted image of the Matterhorn online. It had been encrypted with a block cipher in a particular mode. What mode must it have been CBC, CTR, ECB, or GCM?

9. Mathematically, one of the block cipher modes we covered can be described by the formula $C_n = E_K(P_n \oplus C_{n-1})$, where E_K stands for the encryption algorithm with the key K. What mode is this, CBC, CTR, ECB, or GCM?

10. I have a library of about 5000 songs. One day I put them on shuffle, except it wasn't a true shuffle as songs could be repeated. And indeed I started hearing repeats after about 50 songs. Why?

11. We have a linear congruential generator with $a = 4$, $b = 1$, $m = 13$, and a seed value of 5. Give the first two random numbers generated.

12. Suppose we use AES to encrypt a binary representation of this string: `abcd1234ABCD5678WXYZ1234wxyzABCDabcd5678WXYZ1234`. Assuming each character is one byte in length, how many blocks will this end up being?

13. Someone builds a rig to crack a certain cipher with 48-bit keys. It takes 5 hours to test all the keys. The cipher is then upgraded to 54-bit keys. How long will it take to test all the keys now?

14. Suppose someone builds a rig that is able to test 20 trillion keys a second for a certain cipher. They leave it running nonstop for a year. If the cipher uses 64-bit keys, is it safe, or is it guaranteed to be cracked? Show all your calculations.

15. For this problem, you will be doing an encryption with an 8-bit block cipher. To keep the calculations simple, that block cipher is included in a Python file with this assignment. To encrypt the block 11010001, just do `c('11010001')`. There's no need to change any of the code I wrote. Encrypt the plaintext 00100001111100001010101100000001 in each of the following modes.

    (a) ECB mode

    (b) CBC mode with IV 11100101.

    (c) CTR mode with a 4-bit nonce 0110 and a 4-bit counter.