Homework 2: Block Cipher, Symmetric Cryptography

1. Stream Cipher, Block cipher

(a) Identify each of the following as: a stream cipher (S), or a block cipher (B).

[stream cipher] One-time pad

[stream cipher] Vigenere cipher

[block cipher] AES

(b) A good block cipher exhibits *avalanche effect*: if we flip one bit in the plain text, half of the bits are flipped in the cipher text.

Two messages of the same length, m_1 and m_2, differ by 5 bits. With a good block cipher, how many bits differ in the two resulting cipher texts? Assume both cipher texts are n bits long.

$n/2$ bits.

(c) Generally, block ciphers are slower than stream ciphers.

(d) What advantages do block ciphers have over stream ciphers?

Block ciphers are the building blocks of many modern cryptographic tools:

- Creating pseudo random number (e.g. one-time pads)
- Constructing hash functions
- Creating MACs
- etc.

2. DES and AES

(a) If you are starting a new project that does not depend on other legacy programs, which cipher would you use, 3DES or AES? Justify your answer.

AES.

- It's faster.
- It has a larger key space (mitigates exhaustive search).
- It has a larger block size (therefore the same key can encrypt more messages before it is compromised).

(b) Why is DES broken? Why is 2DES insecure?

The key space of DES is too small (2^{56}), and an inexpensive exhaustive search can be easily done today.

For 2DES, one can launch a meet-in-the-middle attack that reduces the time of an exhaustive search to around 2^{57}, which is significantly smaller than its key space size 2^{112}.

(c) **Bonus**: 3DES is often implemented as E(k_3, D(k_2, E(k_1, m))). Why the decryption in the middle?

This is a hack for backwards compatibility -- if we let $k1 = k2 = k3 = k$ then 3DES($k1$, $k2$, $k3$, m) = DES(k, m).

(d) **Bonus**: both AES and DES use substitution boxes (S-boxes) as part of the encryption algorithm. For which cipher are the S-boxes invertible? Why could you decrypt messages using the other cipher when its S-boxes are non-invertible?
AES's S-boxes are invertible.
DES uses Feistel Network, which doesn't require the S-boxes to be invertible.

3. Block cipher modes

(a) What is the ECB mode? Why should it never ever be used? What modes could you use instead?

Electronic **C**ode **B**ook mode. It always encrypts the same plain text to the same cipher text, thereby leaking information about the plain text to the attacker.

You should use, say, CBC (cipher block chaining) or CTR (randomized counter) modes instead.

Caveat Lector! Improperly using CBC or CTR modes could also result in information leak.

(b) What is a nonce?

It's a number that's never used more than once. Often, but not always, the nonce is randomly generated.