Week of February 11, 2019: Cryptography I

Question 1  *Block Cipher Potpourri*  

(a) What is the difference between IND-KPA and IND-CPA?

(b) Are block ciphers IND-CPA?

(c) What are good possible sources of entropy for key generation for a block cipher?
   - The computer’s clock time (assumed in seconds)
   - The Parent Process ID ⊕ my Process ID ⊕ time
   - Hardware noise generator
   - Hardware noise generator ⊕ time
   - 101010101... ⊕ Hardware noise generator

(d) Why does a block cipher need to be a permutation?
Question 2  *PRNGs and stream ciphers*  

(a) Pretend I have given you a pseudo-random number generator $R$. $R$ is a function that takes a 128-bit seed $s$, an integer $n$, and an integer $m$, and outputs the $m^{th}$ (inclusive) through $m^{th}$ (exclusive) pseudo-random bits produced by the generator when it is seeded with seed $s$. Use $R$ to make a secure symmetric-key encryption scheme. That is, define the key generation algorithm, the encryption algorithm, and the decryption algorithm.

(b) Explain how using a block cipher in counter (CTR) mode is similar to the scenario described above.
Question 3  Block cipher security and modes of operation  (20 min)

As a reminder, the cipher-block chaining (CBC) mode of operation works like this:

The output of the encryption is the ciphertext concatenated with the IV that was used.

(a) Does the initialization vector (IV) have to be non-repeating? Why?

(b) Is a non-repeating IV enough? Imagine you sequentially picked IVs from a list of non-repeating, but publicly-known, numbers, e.g., A Million Random Digits with 100,000 Normal Deviates (RAND, 1955).

Say Alice encrypts the one-block long message $m_1$ with initialization vector $IV_1$ to get $C_1$ and encrypts $m_2$ using $IV_2$ to get $C_2$. She gives these to Mallory and challenges her to tell which $C$ came from which $m$.

Mallory knows that Alice’s next IV will be $IV_3$, and can ask Alice to encrypt messages for her (a chosen plaintext attack). Can Mallory distinguish the two ciphertexts?