Nicholas & Peyrin
Summer 2021

CS 161
Computer Security

Discussion 3

Cryptography I

Question 1 ***Block Cipher and Entropy Potpourri*** ()

(a) Explain how an adversary can always win the IND-CPA game against a deterministic encryption algorithm. Given identical plaintext, a deterministic encryption algorithm will produce identical ciphertext.
(Corollary: AES block cipher and ECB mode of operation, which are deterministic, are IND-CPA insecure.)

(b) Why does a block cipher need to be a permutation?

(c) What are good possible sources of entropy for key generation for a block cipher? Assume a hardware noise generator is a good source of entropy on it's own (these usually incorporate physical sources for randomness).

- The computer's clock time (assumed in seconds)
- The Parent Process ID $\oplus$ my Process ID $\oplus$ time
- Hardware noise generator $\oplus$ a vector of 0s
- Hardware noise generator $\oplus$ time
- Hardware noise generator $\wedge$ a vector of 0s
- Hardware noise generator $\wedge$ time

($\oplus$ and $\wedge$ denote bitwise XOR and AND respectfully)

Question 2 ***PRNGs and stream ciphers*** ()

(a) Suppose you have access to function R that takes a 128-bit seed s and integers n, m as input. R outputs the n^{th} (inclusive) through m^{th} (exclusive) bits produced by the a pseudorandom generator $PRNG$ when it is seeded with seed s.

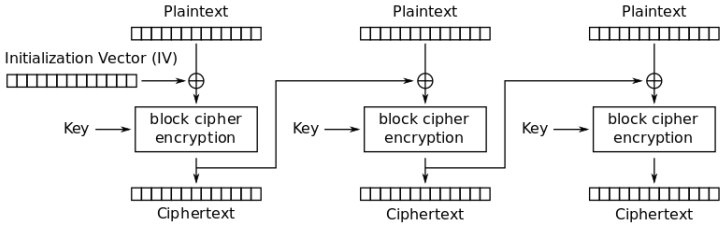
$$R(s, n, m) = PRNG(s)[n : m]$$

Use R to make a secure symmetric-key encryption scheme. That is, define the key generation algorithm, the encryption algorithm, and the decryption algorithm.

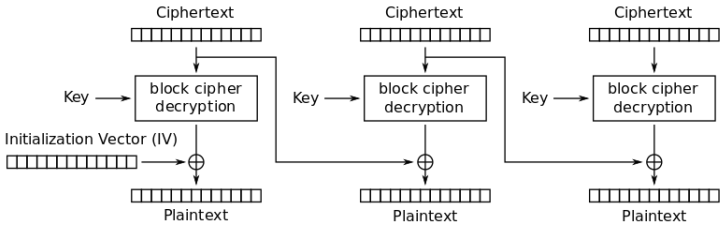
(b) Explain how using a block cipher in counter (CTR) mode is similar to the scenario described above.

Question 3 ***Block cipher security*** ()

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



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

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

(a) What happens if two messages are encrypted with the same key and nonce? What can the attacker learn about the two messages just by looking at their ciphertexts?

(b) If the random number generator used for IV creation is sabotaged, an attacker may be able to predict IVs used to encrypt future data. If this is the case, can an attacker win the IND-CPA game against AES-CBC mode of operation?

Specifically, an attacker provides one-block long plaintext messages P_1 and P_2 to an oracle, which encrypts one of the plaintexts using IV_1.

Can an attacker determine the plaintext used for the first encryption by requesting encryptions of a few chosen plaintexts?

Assume the attacker knows IV_n for any n.