Homework #2

Homework #2

- Chap.6:
  - Review questions 6.7, 6.9, 6.11
  - Problems 6.6(a)(c)
  - Programming problem 6.14*
- Chap.7:
  - Review questions 7.4
  - Problems 7.4, 7.5, 7.8
  - Programming problem 7.19*
- Due: February 22, 2021

- Chap. 6
  - Review question 6.7: Briefly describe ShiftRows.
  - Review question 6.9: Briefly describe MixColumns.
  - Review question 6.11: Briefly describe the key expansion algorithm.

- 6.6 Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.
  (a) XOR of subkey material with the input to the f function.
  (c) f function.

– Programming problem 6.14*: Create software that can encrypt and decrypt using S-AES, as described in Appendix I. Test data: A binary plaintext of 0110 1111 0110 1011 encrypted with a binary key of 1010 0111 0011 1011 should give a binary ciphertext of 0000 0111 0011 1000. Decryption should work correspondingly.

- Chap. 7
  - Review question 7.4: List and briefly define the block cipher modes of operation.
  - Problem 7.4: With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C1 (Figure 7.4) obviously corrupts P1 and P2.

    (a) Are any blocks beyond P2 affected?
    (b) Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

- Problem 7.5: Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?
- Problem 7.8: If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

– Programming Problem 7.19*: Create software that can encrypt and decrypt in cipher block chaining mode using the following cipher: S-DES.

  Test data for S-DES using a binary initialization vector of 1010 1010. A binary plaintext of 0000 0001 0010 0011 encrypted with a binary key of 01111 11101 should give a binary ciphertext of 1111 0100 0000 1011. Decryption should work correspondingly.

- Chap. 8:
  - Review question 8.3: What is the difference between one-time pad and a stream cipher?

– Problem 8.6: What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order.

- Problem 8.9: Suppose you have a true random number generator where each bit in the generated stream has the same probability of being a 0 or 1 as any other bit in the stream and that the bits are not correlated; that is the bits are generated from identical independent distribution. However, the bit stream is biased. The probability of a 1 is $0.5+\partial$ and the probability of a 0 is $0.5-\partial$, where $0< \partial < 0.5$. A simple conditioning algorithm is as follows: Examine the bit stream as a sequence of nonoverlapping pairs. Discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.
  (a) What is the probability of occurrence of each pair in the original sequence?
  (b) What is the probability of occurrence of 0 and 1 in the modified sequence?

- Chap.9:
  - Review Question 9.2: What are the roles of the public and private keys?
  - Review Question 9.4: What requirements must a public-key cryptosystem fulfill to be a secure algorithm?
  -

– Problem 9.4: In an RSA system, the public key of a given user is e=65, n=2881. What is the private key of this user?
Hint: First user trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $\phi(n)$.

- Problem 9.8: Suppose Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A->0, …, Z->25), and then encrypting each number separately using RSA with large e and large n. Is this method secure? If not, describe the most efficient attack against this encryption method.

- Chap. 10:
  - Review question 10.1: Briefly explain Diffie-Hellman key exchange.
  - Problem 10.1: Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=157 and a primitive root α=5.
    (b) If Bob has a private key X_B=27, find his public key Y_B.
  - Problem 10.2: Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=23 and a primitive root α=5.
    (b) If Alice has a public key Y_A=8, what is the shared key with Bob?

Homework Submission

- For hand-written exercises, please scan, convert to compressed pdf and submit to our homework submission site.
- For programming exercises, please submit to our homework submission site.
  - Program uploading: a compressed file (in .zip format) including source codes and compilation instructions if it needs special environment to compile or run
    - Please clearly name your program files using your ID
  - *Note: the uploaded file size must be less than 5MB*