CS 470
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

---

# Homework #1

Due March 25, 2013, 17:00

1. Study the Rijndael (AES) encryption function and the design decisions taken to optimize it in implementation from the handout on the class webpage.

   (a) Explore the general structure of Rijndael. Is it a Feistel cipher? An SP cipher? Why/why not? Explain briefly.

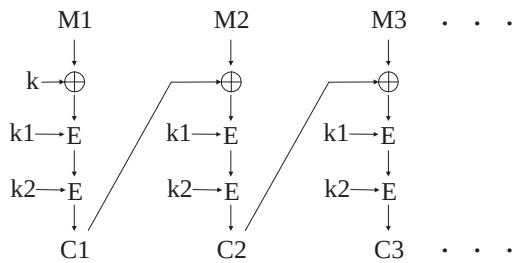
   (b) Explain the functionality of each of the four basic operations, ByteSub, ShiftRow, MixColumn, AddRoundKey in the cipher.

   (c) See how the round function can be implemented by just four table lookups and four XORs on a 32-bit platform. Discuss which properties of the diffusion part make this feature possible. (For instance, would a similar feature be possible if a bit-wise permutation were used for diffusion? Or, if a non-linear operation with no matrix representation were used for MixColumn? Or, what if a "MixRow" similar to MixColumn were used instead of ShiftRow?) Is the same trick applicable on an 8- or 16-bit platform? Why/why not?

   (d) i. Is the performance of the inverse cipher as good as the cipher itself? On a 32-bit platform? On a 8-bit platform?

   ii. Why is the performance of the inverse cipher is not as important as the performance of the cipher itself according to the designers of Rijndael?

2. Consider the following mode of encryption with three keys $k$, $k1$, $k2$, where $k$ is of the length of the block size and $k1$ and $k2$ are of the length of the key size (denoted by $\ell$) of the block cipher $E$. (E.g., for DES, $k$ would be 64 bits, and $k1$ and $k2$ would be 56 bits each.)




   (a) Describe the decryption operation for this mode of encryption.

(b) Describe a known-plaintext attack with a relatively small number of input blocks (e.g., with 20 or 30 blocks) where the attacker can discover the full key $(k, k1, k2)$ with approximately $2 \cdot 2^{\ell}$ runs of the encryption/decryption algorithm. (You can assume as much memory as you need for the attack.)

(c) Comment on the security of this mode of encryption as a potential way of strengthening DES with an increased key size.

3. Answer the following questions regarding the WEP protocol:

(a) Describe the challenge-response authentication protocol used in WEP. Why is this protocol not secure when implemented with a stream cipher like RC4?

(b) Describe the message authentication mechanism used in the WEP protocol. Why is this not secure as a MAC? How can an attacker inject arbitrary packets into the user's connection?

(c) Describe how an active attacker can completely bypass WEP encryption and read WEP-encrypted messages by breaking the MAC scheme used.

4. Suppose that we want to develop a MAC scheme which is as secure as Triple-DES CBC-MAC and at the same time as efficient as Single-DES CBC-MAC. We come up with the following idea: Except the last plaintext block, we apply Single-DES CBC with key $K_1$ and for the last one, we apply 2-key Triple-DES CBC-MAC using keys $(K_1, K_2, K_1)$. The result of the Triple-DES is output as the MAC.

(a) Approximately how many message-MAC pairs would you need to observe in order to find two different messages with the same MAC value?

(b) Describe how an attacker who has observed two different messages with the same MAC value can break this MAC scheme completely by recovering the keys with a time complexity about the same as that of breaking a Single DES encryption.

5. Answer the following questions regarding MD5 and SHA-1:

(a) Note that a message is still padded even if its length is already a multiple of the block length. Why is this important? I.e., what would the problem be if such messages are digested as they are without any padding?

(b) Discuss the relation between these hash functions and the Davies-Meyer construction based on a block cipher.

(c) Why do you think byte operations such as AND, OR, XOR are used instead of S-boxes in the nonlinear $F$ function? What would happen if a structure like the DES $F$ function were used instead of the current functions?