Applied Cryptography

Symmetric Cryptography, Assignment 1, Tuesday, September 10, 2024

Remarks:

- Hand in your answers through Brightspace.
- Hand in format: PDF. Either hand-written and scanned in PDF, or typeset and converted to PDF. Please, **do not** submit photos, Word files, LaTeX source files, or similar. Also submit code used for your assignments (as separate files).
- Assure that the name of **each** group member is **in** the document (not just in the file name).

Deadline: Sunday, September 22, 23.59

1. **(15 points)** A well-known message authentication code not discussed in the lectures is LightMAC. It is defined on top of AES-128 instantiated with two independent and random secret keys K_1, K_2, which we denote as E_{K_1} and E_{K_2}. For $a \in \mathbb{N}$ and $X \in \{0, \ldots, 2^a - 1\}$, $\langle X \rangle_a$ denotes the encoding of X as an a-bit string. We will consider a simplified version of LightMAC (hint: make a drawing of the scheme!):

   - On input of an arbitrary-length message $M \in \{0,1\}^*$, it is padded with a 1 and a sufficient number of 0s so that its length is a positive multiple of 96:

     $$X' \leftarrow M \| 1 \| 0^{-|M|-1 \bmod 96}.$$

     This string is then split into 96-bit blocks $X_1, \ldots, X_\ell$.
   - The ℓ message blocks are concatenated with a counter, and encrypted using E_{K_1}, and the outcome is added into a checksum:

     $$V \leftarrow \bigoplus_{i=1}^{\ell} E_{K_1}(X_i \| \langle i \rangle_{32}).$$

   - The result is encrypted using E_{K_2}, and this gives the tag:

     $$T \leftarrow E_{K_2}(V).$$

   (a) **(3pt)** What is the key size of LightMAC?

   (b) **(4pt)** Is this construction a Wegman-Carter MAC or a Protected Hash MAC?

   Suppose you find two messages M, M' *of the same length* such that LightMAC(M) = LightMAC(M').

   (c) **(3pt)** What can you conclude about the corresponding intermediate values V and V'?

   (d) **(5pt)** Suppose you *additionally* know that, for some known arbitrary-length message X, LightMAC$(M \| 1 \| 0^{-|M|-1 \bmod 96} \| X) = T^\star$. Describe a forgery for LightMAC using this additional knowledge, and explain why this forgery is valid.

2. **(20 points)** In the `PyCryptodome` package, you can find an implementation for `AES-128-ECB`. `AES-128-ECB` applied to a 128-bit input is just the block cipher `AES-128`. Different *modes* can be built using this block cipher, such as `OFB`.

   (a) **(8pt)** Implement `AES-128-OFB` and its inverse using the implementation for `AES-128-ECB`. Remember that in `OFB` mode, the initial value (IV) needs to be random. In particular, your implementation of `AES-128-OFB` needs to take as input a 128-bit value as an IV, and a plaintext which can be of any length. Encrypt a plaintext with an IV and key of your choice, and decrypt the ciphertext again to verify your implementation. The plaintext must be at least 512 bits. Note that the decryption function also takes IV as an input.

(b) **(4pt)** Argue whether `AES-128-OFB` or $\texttt{AES-128-OFB}^{-1}$ can be implemented in parallel.

(c) (**8pt**) Note that in `OFB` mode, it is necessary to use a random IV. Suppose we replace this random IV with a user-chosen nonce N. Explain that this makes the `OFB` mode insecure.

3. **(15 points)** Consider the Wegman-Carter MAC function of lecture 2 slide 14. We have

$$\mathbf{Adv}^{\mathrm{unf}}_{\mathsf{WC}}(q_m, q_v) \leq q_v/2^n + \mathbf{Adv}^{\mathrm{prf}}_{F}(q_m + q_v)\,,$$

provided that the adversary does not query WC_K for repeated nonces.

(a) **(5pt)** Assume you can evaluate this function for repeated nonces. Mount a forgery attack in $q_m = 3$ MAC queries and $q_v = 1$ VFY query.

(b) **(5pt)** Consider the function $H : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ defined as $H_L(M) = L \otimes M$, i.e., defined as finite-field multiplication over $\mathrm{GF}(2^n)$. Prove that H_L is 2^{-n}-XOR-universal.

Hint: Over finite fields, multiplications can be inverted the same way that it can in the field of real numbers. I.e., the equation $A \otimes X = B$ can be solved for X, so long as $A \neq 0$.

(c) **(5pt)** Now, we consider the same setting as in (3a), except that we take the hash function to be the finite-field multiplication of (3b). Describe a forgery attack in only $q_m = 2$ MAC queries and $q_v = 1$ VFY query.