Crypto Engineering
Block ciphers & Hash functions 1

2021-09-28

Exercise 1: No questions

Explain why all of the following statements are wrong.

1. It is never possible to attack an ideal block cipher.
2. A block cipher with keys of 512 bits is always secure.
3. There will never be any reason, technologically speaking, to use (block cipher) keys larger than 128 bits.
4. One should always use (block cipher) keys larger than 128 bits.
5. $*$ IVs of the CBC mode can be generated using `rand48()`
6. $*$ There is no well-analysed and (as far as we know) secure block cipher with larger key sizes than the ones found in the AES family.
7. $*$ One can always use a secure block cipher to build a secure hash function.
8. $*$ One should always use the latest-published, most recent block cipher/hash function.

Exercise 2: CBC ciphertext stealing

This exercise presents an elegant technique to avoid increasing the length of the CBC encryption of a message whose length L is not a multiple of the block size n of the block cipher, as long as $L > n$.

Let $M = m_1 || \cdots || m_{\ell-1} || m_\ell$ be a message of length $L = (\ell-1) \cdot n + r$, where $r = |m_{\ell-1}| < n$. Recall that the CBC encryption of M with the block cipher $\mathcal{E}$ and the key k is $C = c_0 || \cdots || c_\ell$, where c_0 is a random initial value, and $c_i = \mathcal{E}(k, m_i \oplus c_{i-1})$ for $i > 0$.

Q.1 What is the bit length of C, defined above, assuming that m_ℓ is first padded to an n-bit block?

Q.2 Write the decryption equation for one block (that is, explain how to compute m_i in function of c_i, k, and possibly additional quantities).

Let us now rewrite the penultimate ciphertext $c_{\ell-1} = \mathcal{E}(k, m_{\ell-1} \oplus c_{\ell-2})$ as $c'_\ell || P$, where c'_ℓ is r-bit long. We also introduce $m'_\ell = m_\ell || 0^{n-r}$, that is m_ℓ padded with $n - r$ zeros. Finally, let $c'_{\ell-1} = \mathcal{E}(k, m'_\ell \oplus (c'_\ell || P))$.

Q.3 What is the bit length of $C' = c_0 || \cdots || c_{\ell-2} || c'_{\ell-1} || c'_\ell$?

Q.4 Explain how to recover m_ℓ and P from the decryption of $c'_{\ell-1}$, and from there $m_{\ell-1}$ from the one of c'_ℓ.

Exercise 3: An attack on a tweakable block cipher construction

We consider a simple tweakable block cipher construction $\widetilde{\mathcal{E}} : \{0,1\}^\kappa \times \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ that from a (non-tweakable) block cipher $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ defines $\widetilde{\mathcal{E}}(k,t,\cdot) = \mathcal{E}(k \oplus t, \cdot)$. The goal of the exercise is to show the existence of an attack on $\widetilde{\mathcal{E}}$ that runs in time τ (where one time unit corresponds to one evaluation of $\mathcal{E}^\pm$, and memory accesses are free), makes q queries to the oracle $\widetilde{\mathcal{E}}^\pm(k,\cdot,\cdot)$ (i.e. the adversary may obtain encryption (resp. decryption) of chosen plaintexts (resp. ciphertexts) under the unknown key k with a chosen tweak), and recovers k with probability $\approx \min(q\tau/2^\kappa, 1)$.

Q.1

1. We first assume that $\forall x, \mathcal{E}(\cdot, x)$ is injective. Show then that a collision (on the first component) between the lists $L_1 := [(\mathcal{E}(x,0), x) : x \twoheadleftarrow \{0,1\}^\kappa]$ and $L_2 := [(\widetilde{\mathcal{E}}(k,t,0), t) : t \twoheadleftarrow \{0,1\}^\kappa]$ reveals k as $x \oplus t$.
2. Show that this leads to an attack with the same cost as stated above.
3. Do you expect the above assumption to hold if $\kappa = n$? What if $2\kappa = n$?
4. How would you adapt the attack if the above assumption didn't hold?

Exercise 4: An attack on another tweakable block cipher construction (*Exam 2019*)

The goal of this exercice is to describe an attack by Wang et al. (ASIACRYPT 2016) on a tweakable block cipher construction "$\widetilde{\mathcal{F}}[2]$" due to Mennink (FSE 2015).

We will reuse the tweakable block cipher construction $\widetilde{\mathcal{E}}$ from *Exercise 3* and admit the existence of the attack that it describes.

We now define $\widetilde{\mathcal{F}}[2] : \{0,1\}^\kappa \times \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ from a (non-tweakable) block cipher $\mathcal{E}$ in the following way:

1. $y_1 := \mathcal{E}(k,t)$
2. $x_2 := y_1 \oplus p$
3. $y_2 := \mathcal{E}(k \oplus t, x_2)$
4. $c := \widetilde{\mathcal{F}}[2](k,t,p) = y_1 \oplus y_2$

Where y_1, x_2, y_2 are intermediate variables and c is the encryption of p with key k and tweak t. We also assume adversaries given oracle access to $\widetilde{\mathcal{F}}[2]^\pm(k,\cdot,\cdot)$, who can compute $\mathcal{E}^\pm$, and who wish to recover k.

Q.2 Show that $\widetilde{\mathcal{F}}[2]^{-1}(k,0,0) = \mathcal{E}(k,0)$.

Q.3 Show that knowing $\mathcal{E}(k,0)$, an adversary can further recover $\mathcal{E}(k,t)$ for any t, by making the query $\widetilde{\mathcal{F}}[2](k,0,\mathcal{E}(k,0) \oplus t)$

Q.4 Show that it is then possible to obtain $\mathcal{E}(k \oplus t, x)$ for any x by querying $\widetilde{\mathcal{F}}[2](k,t,\mathcal{E}(k,t) \oplus x)$

Q.5 Show how the results of Questions 2 $\sim$ 4 and the existence of an attack on $\widetilde{\mathcal{E}}$ (that can be treated as a black box) leads to an attack on $\widetilde{\mathcal{F}}[2]$. Conclude by explaining how it is possible to recover the key of $\widetilde{\mathcal{F}}[2]$ with probability ≈ 1 with an attack that takes time $2^{\kappa/2}$.

Exercise 5: Davies-Meyer fixed-points

In this exercise, we will see one reason why *Merkle-Damgård strengthening* (adding the length of a message in its padding) is necessary in some practical hash function constructions.

We recall that a compression function $f : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$ can be built from a block cipher $\mathcal{E} : \{0,1\}^b \times \{0,1\}^n \to \{0,1\}^n$ using the "Davies-Meyer" construction as $f(h,m) = \mathcal{E}(m,h) \oplus h$.*

Q.1 Considering the feed-forward structure of Davies-Meyer, under what conditions would you obtain a fixed-point for such a compression function? (That is, a pair (h,m) s.t. $f(h,m) = h$.)

Q.2 Show how to compute the (unique) fixed-point of $f(\cdot,m)$ for a fixed m. Given h, is it easy to find m such that it is a fixed-point, if $\mathcal{E}$ is an ideal block cipher?

Q.3 A *semi-freestart collision attack* for a Merkle-Damgård hash function $\mathcal{H}$ is a triple (h,m,m') s.t. $\mathcal{H}_h(m) = \mathcal{H}_h(m')$, where $\mathcal{H}_h$ denotes the function $\mathcal{H}$ with its original IV replaced by h. Show how to use a fixed-point to efficiently mount such an attack for Davies-Meyer + Merkle-Damgård, when strengthening is not used.

Note: Fixed-points of the compression function can be useful to create the *expandable messages* used in second preimage attacks on Merkle-Damgård.

*Here, the feedforward uses bitwise XOR, but alternatives exist.