Crypto Engineering
Block ciphers & Hash functions 1

2018-09-28

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: 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.

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

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

Exercise 3: 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.