Cryptology I (spring 2020) Dominique Unruh

Exercise Sheet 6

Out: 2020-04-07 Due: 2020-04-15

Problem 1: Hash functions

Let E be a block cipher with key and block length n. Let $F(x\|y) := E(x, y)$ (the compression function). Let H be the Merkle-Damgård construction using F as compression function.

(a) Show how to find a collision for F.

(b) Show how to find a collision for H.

Note: If finding a collision for H is too difficult, you might first try to find a collision for H when H is constructed using the Iterated Hash construction. (This will give points, too.) In this case, however, the colliding messages have to have the same length.

Problem 2: Authentication in WEP (bonus problem)

In the WEP-protocol (used for securing Wifi, now mostly replaced by WPA), messages are "encrypted" using the following procedure: First, a key k is established between the parties A and B. (We do not care how, for the purpose of this exercise we assume that this is done securely.) Then, to transmit a message m, A chooses an initialization vector IV (we do not care how) and sends IV and $c := \mathit{keystream} \oplus (m\|\mathit{CRC}(m))$. Here *keystream* is the RC4 keystream computed from IV and k (we do not care how).

The function CRC is a so-called cyclic redundancy check, a checksum added to the WEP protocol to ensure integrity. We only give the important facts about CRC and omit a full description. Each bit of $\mathit{CRC}(m)$ is the XOR of some of the message bits. Which messages bits are XORed into which bit of $\mathit{CRC}(m)$ is publicly known. (In other words, the i-th bit of $\mathit{CRC}(m)$ is $\bigoplus_{j\in I_i} m_j$ for a publicly known I_i.)

An adversary intercepts the ciphertext c. He wishes to flip certain bits of the message (i.e., he wants to replace m by $m \oplus p$ for some fixed p). This can be done by flipping the corresponding bits of the ciphertext c. But then, the CRC will be incorrect, and B will reject the message after decryption! Thus the CRC *seems* to ensure integrity of the message and to avoid malleability. (This is probably why the designers of WEP added it here.)

Show that the CRC does not increase the security! That is, show how the adversary can modify the ciphertext c such that c becomes an encryption of $m \oplus p$ and such that the CRC within c is still valid (i.e., it becomes the CRC for $m \oplus p$).

Hint: Think of how the i-th bit of $CRC(m \oplus p)$ relates to the i-th bit of $CRC(m)$. (Linearity!)

Problem 3: Collisions in Iterated Hash

Let E be a block cipher with n-bit keys and messages. Assume the following compression function:

$$F(x\|y) := E(y, x) \oplus x.$$

(y is used as the key for E.) This is a very slight variation of the Davies-Meyer compression function.

Let H be the Iterated Hash construction using compression function F.

Assume the designer of the standard happens to have chosen the initialization vector iv as $iv := D(z, 0)$ for random z. (Here D is the decryption corresponding to E.) The designer justified this with the fact that this basically leads to a random iv.

Describe how to (efficiently) find a collision for H.

Note: You can assume that you know which z the designer used.

Hint: First explain how to efficiently construct x^* as describe in the lecture in the attack on Iterated Hash.

Problem 4: Birthday attack

Implement a birthday attack for a hash function with 48 bit output. The python code in `birthday.py` contains template code, fill in the code for the function `find_collision`.