Homework sheet 3, due 12 December 2019 at 13:30

Submit your homework (text and code) by encrypted and signed email to all three TAs. Make sure to test early whether your encryption program can handle Jonathan's key and if not, contact him for an alternative. Do not forget to attach your public key and the public key of anybody you put in cc. Make sure to have different members of your group handle the submission. Do not forget to attach your public key if we don't have it yet.

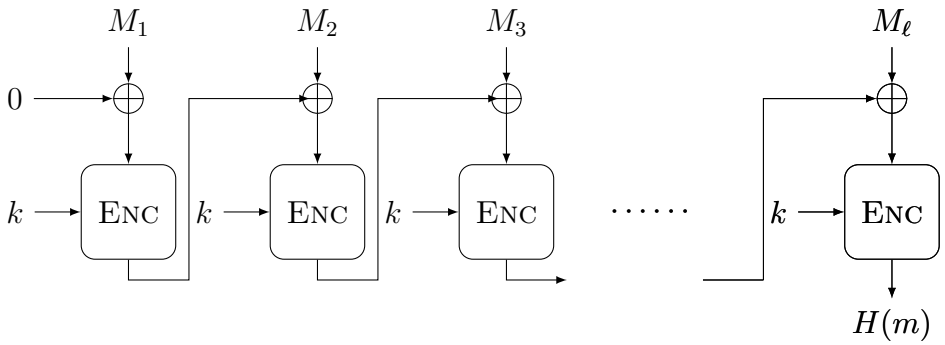
1. In SSLv3 one of the two options for symmetric encryption is DES in CBC mode. To protect against message forgery a message authentication code MAC is used. SSLv3 uses the MAC-then-encrypt approach, thus a message m first gets encoded as $M = m||\text{MAC}(m)||\text{pad} = M_1 \dots M_{\ell-1} M_\ell$ and then encrypted using DES with CBC. The padding pad is chosen so that the total length of M in bytes is a multiple of 8 (to match the block size of DES) and that the last byte states the length of the padding (including this byte) in bytes. Note, the latter means that there always has to be a padding, even if $m||\text{MAC}(m)$ has length a multiple of 8. There are no further requirements on how the padding is chosen. Upon receiving a ciphertext C, a computer will decrypt the message M, read the last byte to learn the length of the padding to identify m and MAC(m), and finally verify the MAC. If this verification fails the computer will close the connection.

   (a) Just as a reminder of how CBC works, state the formula for decrypting the last block of the ciphertext. | 1 point |

   (b) Assume that $C = C_0 C_1 \dots C_{\ell-1} C_\ell$ is a ciphertext so that the C_ℓ block comes entirely from the encryption of pad. The first block C_0 equals the IV. What is the value of the last byte in M_ℓ? Show how this gives you a method that for each $0 < i < \ell$ you can test whether the last byte of M_i matches a publicly available value (computed from the C_i).

   To give a concrete example let C_0 =`01 23 45 67 89 AB CD EF`, $C_{\ell-1}$ =`12 34 56 78 9A BC DE F0` (in hex) and (like above) let C_ℓ come entirely from padding. What value of the last byte of M_1 can you test for? | 13 points |

2. Inspired by the Merkle-Damgård construction and block cipher modes, cryptographer Charlie constructs a hash function digesting message $m = (M_1, m_2, M_3, \dots, M_\ell)$ block wise to $H(m)$ using a modification of CBC encryption. The key k is publicly known and fixed, the $IV = 0$ is publicly known and fixed. Each M_i and the key have the correct block length n for the block cipher Enc: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Charlie's hash function computes $H(m)$ as follows:



(Picture credit: Modified from CBC encryption by Diana Maimut.)

(a) Show how to break preimage resistance, i.e. given $y \in \{0,1\}^n$ find a preimage $x \in \{0,1\}^*$ with $H(x) = y$. | 2 points |

(b) Show how to break second preimage resistance, i.e. given $x \in \{0,1\}^*$ find $x' \neq x$ with $H(x) = H(x')$. | 2 points |

(c) Show how to break collision resistance, i.e. find $x, x' \in \{0,1\}^*$ with $x \neq x'$ so that $H(x) = H(x')$. | 2 points |