## Homework sheet 4, due 16 December 2021 at 13:30

Submit your homework (pdf and code, if any) by encrypted and signed email to all TAs (not Tanja). 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.

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 $M = m||\text{MAC}(m)||\text{pad} = M_0 \ldots M_{t-1}$ 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 $\text{MAC}(m)$, 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 C_{t-1} of the ciphertext. $\boxed{\text{1 point}}$

   (b) Assume that $C = \text{IV} C_0 C_1 \ldots C_{t-1}$ is a ciphertext so that the C_{t-1} block comes entirely from the encryption of pad. What is the value of the last byte in M_{t-1}? $\boxed{\text{2 points}}$

   (c) In the situation of (b), show how this gives you a method that for each $0 < i < t - 1$ allows you to test whether the last byte of M_i matches a publicly available value (computed from the C_is).
   Hint: you need all pieces provided in the next part to get the value you can test for in M_0. Of course the attack also needs C_0 but that does not influence the value you can check for. Here you should state things for M_i with general i. $\boxed{\text{8 points}}$

   (d) In the situation of (b), use the attack you found in (c) on the followinng concrete example: let IV $=$01 23 45 67 89 AB CD EF, C_{t-2} $=$12 34 56 78 9A BC DE F0 (in hex) and (like above) let C_{t-1} come entirely from padding. What value of the last byte of M_0 can you test for? $\boxed{\text{3 points}}$

2. Inspired by the Merkle-Damgård construction and block cipher modes, cryptographer Charlie constructs a hash function digesting message $m = (M_0, M_1, M_2, \ldots, M_{t-1})$ 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 has the correct block length n for the block cipher Enc: $\{0, 1\}^n \times \{0, 1\}^\ell \to \{0, 1\}^n$. Charlie's hash function computes $H(m)$ as follows:
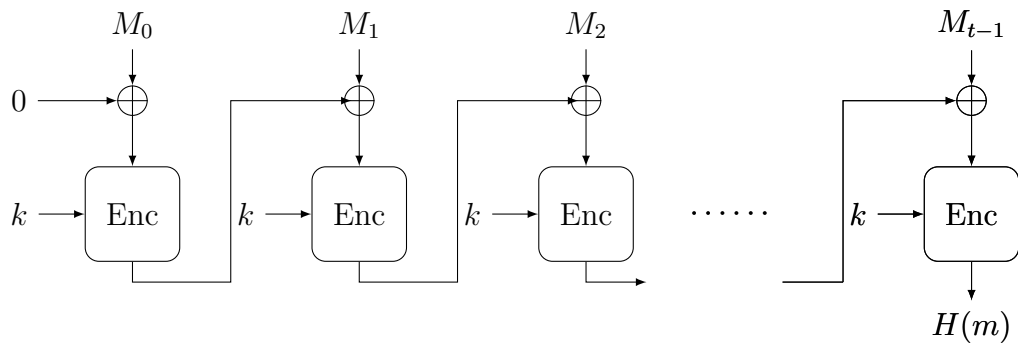
(Picture credit: Modified from CBC encryption by Diana Maimut.)

(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