Applied Cryptography Mid-term Examination

Spring Semester 2021

(263-4660-00L)

K.G. Paterson

Examination Rules:

(a) Written exam, 75 minutes total.

(b) This an open book exam. You have to complete it on your own, without communicating with any other person, but you are permitted to consult textbooks, lecture notes, the world wide web, etc.

(c) If you feel disturbed or have questions about the exam, use the "raise hand" feature in Zoom to call an assistant.

(d) Show all your work. For some questions, you may get partial credit even if the end result is wrong due to a calculation mistake.

(e) There are 3 parts of the exam, worth 25 marks each. You should attempt them all.

(f) You can make free use of mathematical notation and latex-style conventions in your answers. For example "^" can be used to indicate a superscript or a power, "_" for subscript, "`XOR`" for XOR etc. Make sure to use brackets to ensure any mathematical expressions are unambiguous.

Moodle exam details:

(a) The exam has 10 pages (excluding this one).

(b) You can go back and forth using either quiz navigation on the right, or the "Previous page" and "Next page" buttons at the bottom.

(c) Every time you hit a button in "quiz navigation", "Previous page", or "Next page", your answers are autosaved. Every 1 minute your answers are autosaved.

Emergency contact:
In case of any emergency please call immediately (!): +41 44 632 74 16 or contact us via email: mia.filic@inf.ethz.ch.

Problem 1 (MACs).

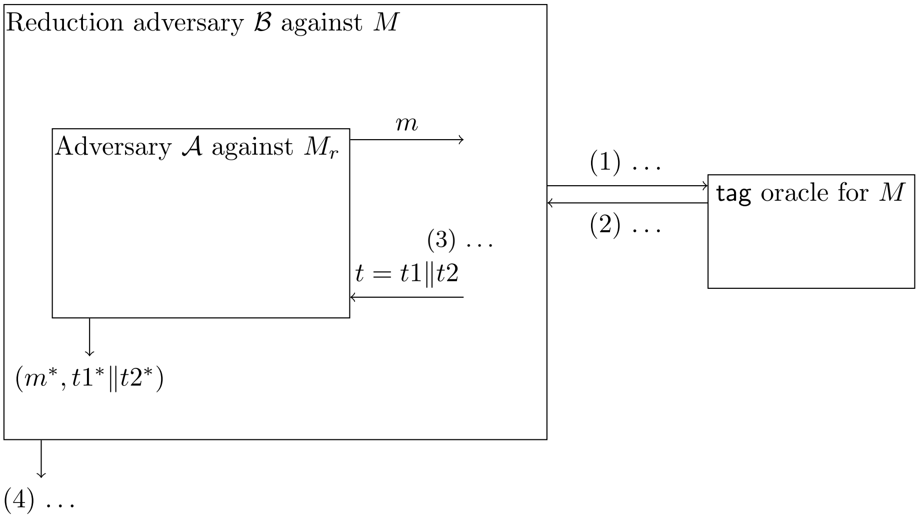
(a) Building an SUF-CMA MAC from another SUF-CMA MAC

Let $M := (\mathsf{KGen}, \mathsf{Tag}, \mathsf{Vfy})$ be a deterministic SUF-CMA secure MAC scheme with tag-length n bits.

Let $M_r := (\mathsf{KGen}, \mathsf{Tag_r}, \mathsf{Vfy_r})$ be a MAC scheme with

$$\mathsf{Tag_r}(K, m) := \mathsf{Tag}(K, m) || 0^n.$$

1) Define the algorithm $\mathsf{Vfy_r}(K, m, t = t1||t2)$ such that M_r is SUF-CMA secure (you may use the decomposition $t = t1||t2$ for the two halves of a $2n$-bit tag of M_r).
2) Briefly and informally argue why M_r is SUF-CMA secure (assuming M is SUF-CMA secure).
3) Prove that if M is SUF-CMA secure, then M_r is SUF-CMA secure by filling the gaps in the following reduction adversary $\mathcal{B}$ using an adversary $\mathcal{A}$ against the SUF-CMA security of M_r (fill in the four marked blanks (1)–(4) in the picture) and provide the resulting reduction advantage in term's of $\mathcal{A}$'s advantage which you may abbreviate as Adv(A) $= Adv_{M_r}^{SUF\text{-}CMA}(\mathcal{A})$.


Reduction adversary $\mathcal{B}$ against M
Adversary $\mathcal{A}$ against M_r
m
(1) ...
tag oracle for M
(2) ...
(3) ...
$t = t1||t2$
$(m^*, t1^*||t2^*)$
(4) ...

(b) Combining two MACs

Let $M1 := (\mathsf{KGen1}, \mathsf{Tag1}, \mathsf{Vfy1})$ and $M2 := (\mathsf{KGen2}, \mathsf{Tag2}, \mathsf{Vfy2})$ be deterministic SUF-CMA secure MAC schemes, both with tag-length $2n$.

Define a MAC scheme $M_c := (\mathsf{KGen_c}, \mathsf{Tag_c}, \mathsf{Vfy_c})$ that combines two halves from each of $M1$ and $M2$'s tags into a new tag as follows:

```
$\underline{\mathsf{KGen_c}()}$
$(K1, K2) \leftarrow\!\!\$\ (\mathsf{KGen1}(), \mathsf{KGen2}())$
Return $(K1, K2)$


$\underline{\mathsf{Tag_c}((K1, K2), m)}$
$t \leftarrow \mathsf{Tag1}(K1, m)[1..n] \parallel \mathsf{Tag2}(K2, m)[n+1..2n]$
Return $t$


$\underline{\mathsf{Vfy_c}((K1, K2), m, t)}$
$a1 \leftarrow (\mathsf{Tag1}(K1, m)[1..n] = t[1..n])$
$a2 \leftarrow (\mathsf{Tag2}(K2, m)[n+1..2n] = t[n+1..2n])$
Return $(a1 \wedge a2)$
```

(where $s[i..j]$ indicates the substring from bits i through j of a bit string s.

4) Give SUF-CMA secure example schemes $M1, M2$ and an adversary $\mathcal{A}$ that perfectly breaks SUF-CMA security of M_c when built from those example schemes $M1, M2$, i.e., with advantange probability $Adv^{SUF\text{-}CMA}_{M_c}(\mathcal{A}) = 1$. Briefly explain why $\mathcal{A}$ is always successful. You may assume that some message called m^* is in the message space.

5) (SUF-CMA vs. WUF-CMA security) Given the following code-based definition of **strong** unforgeability under chosen-message attacks (SUF-CMA) security for a MAC scheme $M = (\mathsf{KGen}, \mathsf{Tag}, \mathsf{Vfy})$, describe which lines you have to change and how to change them to obtain the game for **weak** unforgeability under chosen-message attacks (WUF-CMA) security.

   In your answer, just state the new version of lines with line numbers, for example like this, replacing lines 1 and 5 with the respective code:

   1. $K \leftarrow\!\!\$\ 0^n$
   5. Return true

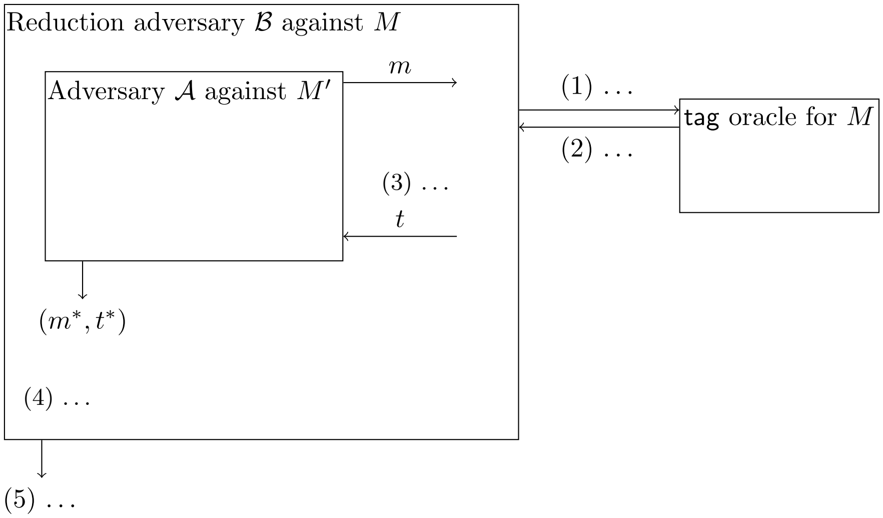
```
Game $\mathbf{SUF\text{-}CMA}(\mathcal{A}, M)$:
1  $\mathsf{K} \leftarrow\!\!\$\ \mathsf{KGen}()$
2  $S \leftarrow \emptyset$
3  $(m^*, t^*) \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{tag}}()$
4  $\mathsf{win} \leftarrow \mathsf{Vfy}(\mathsf{K}, m^*, t^*)$ AND $((m^*, t^*) \notin S)$
5  Return $\mathsf{win}$

Oracle $\mathsf{tag}(m)$:
6  $t \leftarrow \mathsf{Tag}(K, m)$
7  $S \leftarrow S \cup \{(m, t)\}$
8  Return $t$
```

6) (MAC: Separating SUF-CMA and WUF-CMA) Given a WUF-CMA MAC scheme $M = (\mathsf{KGen}, \mathsf{Tag}, \mathsf{Vfy})$, define a MAC scheme $M' =$

$(\mathsf{KGen}', \mathsf{Tag}', \mathsf{Vfy}')$ which is WUF-CMA secure but not SUF-CMA secure.

7) Prove that if M is WUF-CMA secure, then M' is WUF-CMA secure by filling the gaps in the following reduction adversary $\mathcal{B}$ using an adversary $\mathcal{A}$ against the WUF-CMA security of M'.


Reduction adversary $\mathcal{B}$ against M
Adversary $\mathcal{A}$ against M'
m
(1) ...
tag oracle for M
(2) ...
(3) ...
t
(m^*, t^*)
(4) ...
(5) ...

8) Explain in your own words why the reduction above doesn't similarly work to show that SUF-CMA security of M implies SUF-CMA security of M'.

9) Specify an adversary $\mathcal{A}$ that breaks the SUF-CMA security of M' with advantage 1. You may assume that some message called m^* is in the message space.

Problem 2 (AE).

(a) Hash-then-Encrypt with CTR mode

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a PRP-secure block cipher. Defining $B := \{0,1\}^n$, let $SE_{CTR} := (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be the symmetric encryption scheme with keyspace $\{0,1\}^k$, message space $B^{\leq L+1}$ and ciphertext space $B^{\leq L+2}$ that uses E in "CTR mode" (Counter mode) with the initial counters chosen uniformly at random from B $(= \{0,1\}^n)$ and placed as the first ciphertext block.

Using a collision-resistant hash function $H : B^{\leq L} \to B$, we construct a symmetric encryption scheme $SE_{CTR}^{HtE} := (\mathsf{KGen}, \mathsf{Enc}^{HtE}, \mathsf{Dec}^{HtE})$ with message space $B^{\leq L}$ and ciphertext space $B^{\leq L+2}$ via the following generic

”Hash-then-Encrypt” (HtE) approach. (In the description of Dec^{HtE} below, t is a single block, i.e., $t \in B$.)

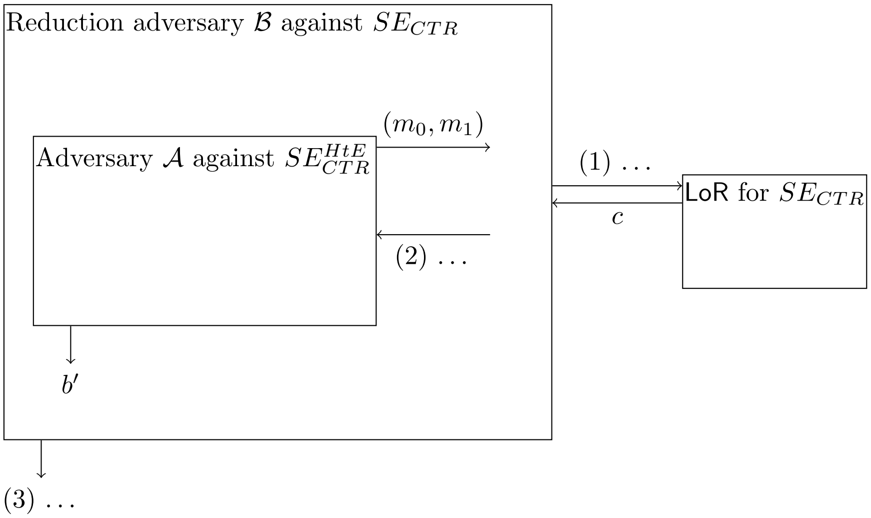
Description of a ”Hash-then-Encrypt” construction that uses an underlying CTR-mode encryption.

```
$\mathsf{Enc}^{HtE}(\mathsf{K}, m)$
$c \leftarrow \mathsf{Enc}(\mathsf{K}, H(m) \,\|\, m)$
Return $c$

$\mathsf{Dec}^{HtE}(\mathsf{K}, c)$
$t \,\|\, m \leftarrow \mathsf{Dec}(\mathsf{K}, c)$
If $t \neq H(m)$ then
    Return $\perp$
Else return $m$
```

10) Taking n to be sufficiently large, we know that $SE_{CTR} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure while relying on the PRP-security of E.

    Prove that SE^{HtE}_{CTR} is IND-CPA secure by filling the numbered gaps on specific arrows in the following diagram depicting a reduction adversary $\mathcal{B}$ that uses an adversary $\mathcal{A}$ against the IND-CPA security of SE^{HtE}_{CTR}, and provide the resulting reduction advantage in terms of $\mathcal{A}$'s advantage which you may abbreviate as Adv(A) $= Adv^{\text{IND-CPA}}_{SE^{HtE}_{CTR}}(\mathcal{A})$.


Reduction adversary $\mathcal{B}$ against SE_{CTR}
(m_0, m_1)
Adversary $\mathcal{A}$ against SE^{HtE}_{CTR}
(1) . . .
LoR for SE_{CTR}
c
(2) . . .
b'
(3) . . .

    Give an informal explanation of why the reduction works.

11) Prove that SE^{HtE}_{CTR} is not IND-CCA secure by filling the gaps in specific lines of the following pseudocode corresponding to an adversary $\mathcal{A}$ so that it breaks the IND-CCA security of SE^{HtE}_{CTR} with a high probability. Explain informally why $\mathcal{A}$'s attack works and provide a lower bound on $\mathcal{A}$'s advantage, clearly stating any assumptions you make in your analysis.

(The LoR oracle below is as defined in the IND-CPA game w.r.t. SE^{HtE}_{CTR}.)

```
Adversary $\mathcal{A}^{\mathsf{LoR},\mathsf{dec}^{HtE}}$:
Pick two distinct messages
$m_0 \in B$ and $m_1 \in B$
$c \leftarrow \mathsf{LoR}(m_0, m_1)$
Parse $c$ as $c_0 \parallel c_1 \parallel c_2$
$c'_0 \leftarrow \dots$
$c'_1 \leftarrow \dots$
$c'_2 \leftarrow \dots$
$\vdots$
$c' \leftarrow c'_0 \parallel c'_1 \parallel c'_2$
$m' \leftarrow \mathsf{dec}^{HtE}(c')$
If ... then:
    Return 0
Else return 1
```

12) Does SE^{HtE}_{CTR} provide INT-CTXT security? Give an informal explanation of your answer.

(b) Hash-then-Encrypt with CBC mode

Let $SE_{CBC} := (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be the symmetric encryption scheme with keyspace $\{0,1\}^k$, message space $B^{\leq L+1}$ and ciphertext space $B^{\leq L+2}$ that uses the block-cipher E in "CBC mode" (Cipher Block Chaining mode) with the uniformly random IV placed as the first ciphertext block.

Using SE_{CBC} and hash function H, we construct a symmetric encryption scheme $SE^{HtE}_{CBC} := (\mathsf{KGen}, \mathsf{Enc}^{HtE}, \mathsf{Dec}^{HtE})$ with message space $B^{\leq L}$ and ciphertext space $B^{\leq L+2}$ via a slight variant of the previous generic "Hash-then-Encrypt" (HtE) approach, where this time the hash of the message is placed as a **suffix** (instead of a prefix) of the plaintext. We also use the Enc, Dec algorithms of SE_{CBC} instead of those of SE_{CTR}. (In the description of Dec^{HtE} below, t is a single block, i.e., $t \in B$.)

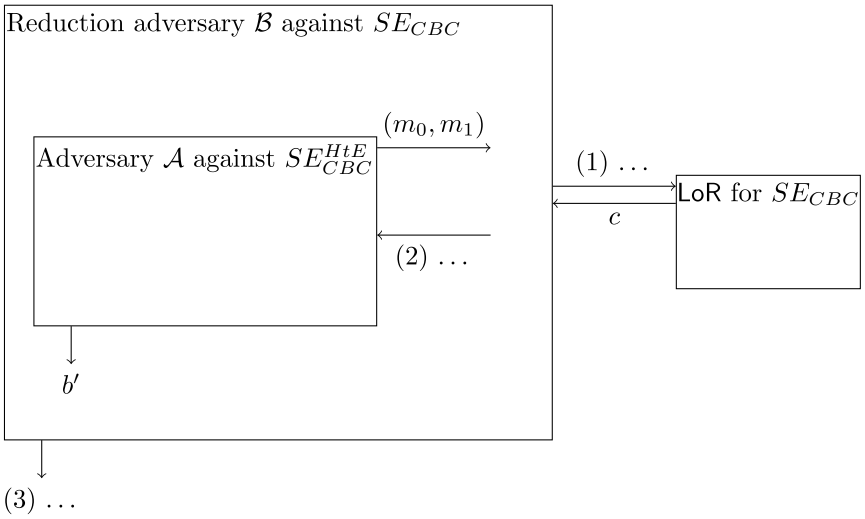
```
$\mathsf{Enc}^{HtE}(K, m)$
$c \leftarrow \mathsf{Enc}(K, m \parallel H(m))$
Return $c$

$\mathsf{Dec}^{HtE}(K, c)$
$m \parallel t \leftarrow \mathsf{Dec}(K, c)$
If $t \neq H(m)$ then
    Return $\perp$
Else return $m$
```

13) Taking n to be sufficiently large and generating IVs uniformly at random, it can be shown that $SE_{CBC} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure under the assumption that E is a PRP.

Prove that SE^{HtE}_{CBC} is IND-CPA secure by filling the numbered gaps on specific arrows in the following diagram depicting a reduction adversary $\mathcal{B}$ that uses an adversary $\mathcal{A}$ against the IND-CPA security of SE^{HtE}_{CBC}, and provide the resulting reduction advantage in terms of $\mathcal{A}$'s advantage which you may abbreviate as Adv(A) = $Adv^{\text{IND-CPA}}_{SE^{HtE}_{CBC}}(\mathcal{A})$.

Give an informal explanation of why the reduction works.


Reduction adversary $\mathcal{B}$ against SE_{CBC}
Adversary $\mathcal{A}$ against SE_{CBC}^{HtE}
(m_0, m_1)
(1) . . .
LoR for SE_{CBC}
c
(2) . . .
b'
(3) . . .

14) Prove that SE_{CBC}^{HtE} is not IND-CCA secure by filling the gaps in specific lines of the following pseudocode corresponding to an adversary $\mathcal{A}$ so that it breaks the IND-CCA security of SE_{CBC}^{HtE} with a high probability.

Your adversary should select two 2-block messages m_0 and m_1. Explain informally why $\mathcal{A}$'s attack works and provide a lower bound on $\mathcal{A}$'s advantage, clearly stating any assumptions you make in your analysis.

(The LoR oracle below is as defined in the IND-CPA game w.r.t. SE_{CBC}^{HtE}.)

```
Adversary $\mathcal{A}^{\mathsf{LoR},\mathsf{dec}^{HtE}}$:
  $m_0 \leftarrow \ldots \,\|\, \ldots$
  $m_1 \leftarrow \ldots \,\|\, \ldots$
  $c \leftarrow \mathsf{LoR}(m_0, m_1)$
  Parse $c$ as $c_0 \,\|\, c_1 \,\|\, c_2 \,\|\, c_3$
  $c'_0 \leftarrow \ldots$
  $c'_1 \leftarrow \ldots$
  $c'_2 \leftarrow \ldots$
  $\vdots$
  $c' \leftarrow c'_0 \,\|\, c'_1 \,\|\, c'_2$
  $m' \leftarrow \mathsf{dec}^{HtE}(c')$
  If $\ldots$ then:
      Return 0
  Else return 1
```

15) Does SE_{CBC}^{HtE} provide INT-CTXT security? Give an informal explanation of your answer.

Problem 3 (Merkle-Damgård construction).

(a) Merkle-Damgård construction using Davies-Meyer compression function

This question concerns the Merkle-Damgård (MD) construction of a hash function from a compression function, where the compression function is built from a block cipher using the Davies-Meyer method.

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with a k-bit key and an n-bit block.

16) (Insecure variant of Davies-Meyer) Let $h_0(t,m) = \mathsf{E}(m,t)$ for $t \in \{0,1\}^n$ and $m \in \{0,1\}^k$. Show that constructing second pre-images for h_0 is trivial, i.e. show that given (t_0, m_0) it is easy to find $(t_1, m_1) \neq (t_0, m_0)$ such that:

$$h_0(t_0, m_0) = h_0(t_1, m_1).$$

17) (The Davies-Meyer compression function) Let $h(t,m) := \mathsf{E}(m,t) \oplus t$ for $t \in \{0,1\}^n$ and $m \in \{0,1\}^k$. Describe a method that, for any choice of $m \in \{0,1\}^k$, constructs a value $t \in \{0,1\}^n$ such that:

$$h(t,m) = t.$$

Such a value t will be referred to henceforth as a fixed point for h.

18) Now consider the use of h as defined above to construct a hash function H using Merkle-Damgård construction; Suppose $m = m_1 m_2 \ldots m_\ell$ consists of ℓ blocks m_i, each block consisting of k bits. Let $IV \in \{0,1\}^n$ be a fixed initialisation vector. Define:

$$t_i := h(t_{i-1}, m_i) \quad i = 1, \ldots, \ell$$

where $t_0 := IV$. Set $H(m) = t_\ell$. (Note that this definition of H does not involve any padding or length encoding.)

Suppose that when computing $H(m)$ on some input $m = m_1 m_2 \ldots m_\ell$, the value t_i is found to be a fixed point for h, i.e., $h(t_i, m^*) = t_i$ for some k-bit block m^*. Given (an integer) $r \geq 1$, show how to efficiently construct a second pre-image m' for m under H such that m' has $\ell + r$ blocks.

19) Suppose m is a message of length $\ell = 2^{n/2}$ blocks (each block consisting of k bits). Show that, with constant probability (which you do not have to derive), it is possible to construct a second pre-image m' for m under H using $\mathcal{O}\left(2^{n/2}\right)$evaluations of h and $\mathcal{O}\left((n+k)2^{n/2}\right)$ bits of storage, such that m' has $\ell + r$ blocks for any $r \geq 1$. State any assumptions you use in your analysis.

(Hint: Consider how to construct many different fixed points t and how these might interact with chaining values t_i arising when computing $H(m)$. Then use your answer to the previous part.)

(b) Merkle-Damgård Davies-Meyer construction with encoding

Now consider the Merkle-Damgård-strengthened version of H, namely $H_{\texttt{MD}}$. Recall that the Merkle-Damgård (MD) construction involves encoding message before hashing, by adding padding and a length field. For simplicity, we will assume that all messages (before encoding) consist of a whole number of k-bit blocks. Then, if $m = m_1 m_2 \ldots m_\ell$ consists of ℓ such blocks m_i, we have:

$$H_{\texttt{MD}}(m) = H(\texttt{encode}(m))$$

where

$$\texttt{encode}(m) = m_1 \ldots m_\ell m_{\ell+1}$$

and $m_{\ell+1}$ consists of "one-zero" bit padding followed by a d-bit encoding of the length of m (in bits) for some fixed value of d. Here we assume d is bigger than $n/2+1$, so that long messages can be hashed.

20) Explain why your previous attack on second pre-image resistance no longer applies to $H_{\texttt{MD}}$.

21) Suppose that m (in unencoded form) has $\ell = 2^{(n/2)+1}$ blocks m_i. So $\texttt{encode}(m) = m_1 \ldots m_\ell m_{\ell+1}$ where $m_{\ell+1}$ contains padding and length encoding. Define $t_i := h(t_{i-1}, m_i)$ for $i = 1, \ldots, \ell+1$, where $t_0 := IV$. So we have $H_{\texttt{MD}}(m) = t_{\ell+1}$.
Let $m'_1, \ldots, m'_{(\ell/2)-1}$ be $(\ell/2)-1$ random k-bit blocks.

Show how to construct, with constant success probability, an $(\ell/2)$-block message m' such that the first $(\ell/2)-1$ blocks equal the blocks m'_i and such that $H(m') = t_j$ for some j with $\ell/2 + 1 \leq j \leq \ell$. Your construction should use $\mathcal{O}(2^{(n/2)})$ evaluations of h and $\mathcal{O}((n+k)2^{(n/2)})$ additional bits of storage. State clearly any assumptions you make.

22) Consider the values t'_j defined via $t'_j := h(t'_{j-1}, m'_i)$ for $j = 1, \ldots, \ell/2$, where $t'_0 := IV$.
Show that, with constant probability, at least one of these values is a fixed point for h, i.e., there exists a message block m^* such that $t'_p = h(t'_p, m^*)$ for some index p. Explain how to identify a suitable value p and message block m^*.

(Hint: You solved a very similar problem in Question 19).)

23) By combining your answers to Questions 21) and 22), show how to construct a second pre-image for m under $H_{\texttt{MD}}$ using $\mathcal{O}(2^{n/2})$ evaluations of h, $\mathcal{O}((n+k)2^{n/2})$ bits of storage, and constant success probability.
What can you deduce about the second pre-image resistance of $H_{\texttt{MD}}$ in comparison to what is expected for generic attacks?