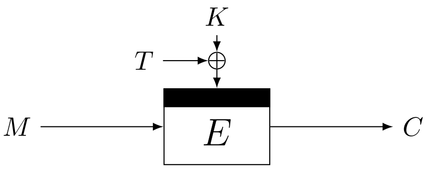
Applied Cryptography

Symmetric Cryptography, Assignment 2, Monday, February 19, 2024

Exercises with answers and grading.

1. **(10 points)** Consider a tweakable block cipher $\widetilde{E} : \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, a tweakable block cipher taking a k-bit key, k-bit tweak and n-bit data, built from an n-bit block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ as follows:



It is possible to recover the secret key K with high probability, by making $2^{k/2}$ evaluations of $\widetilde{E}_K$ and $2^{k/2}$ offline evaluations of E. Explain how. Here, you may assume that $k \ll n$, i.e., that k is much smaller than n.

Hint: Can you find some kind of collision?

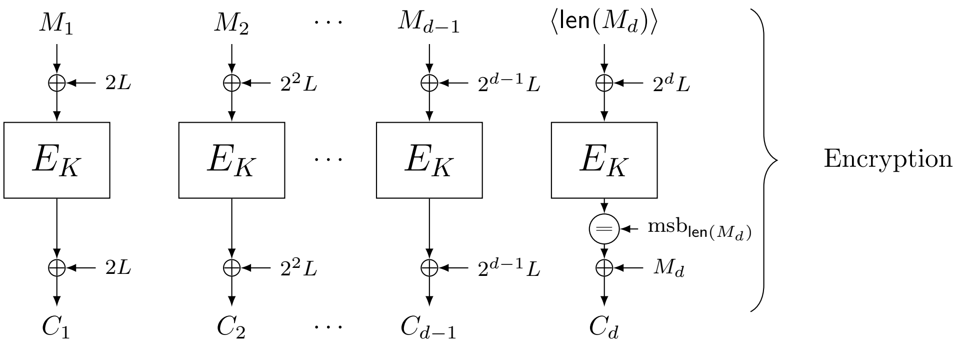
Begin Secret Info:...
Let $q = 2^{k/2}$. The attacker makes the following queries:

- *q construction queries $(T_i, 0) \mapsto C_i = \widetilde{E}_K(T_i, 0)$ for varying T_i;*
- *q primitive queries $(L_j, 0) \mapsto Y_j = E_{L_j}(0)$ for varying L_j;*
- *If there exist i, j such that $C_i = Y_j$, then the key satisfies $K = T_i \oplus L_j$.*

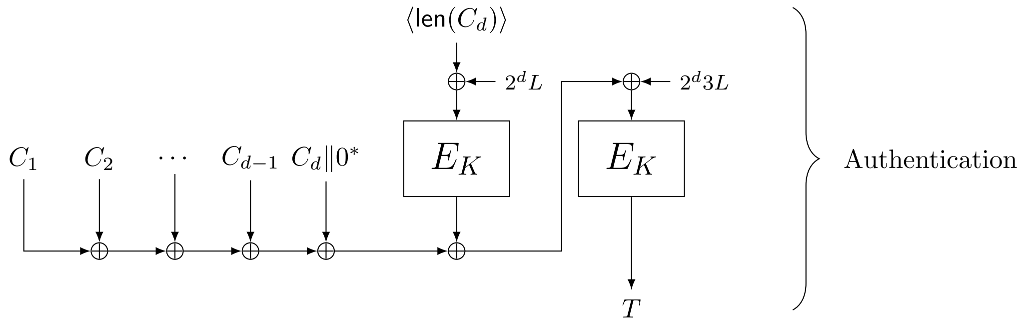
As $k \ll n$, the probability that the collision $C_i = Y_j$ happens even though $K \neq T_i \oplus L_j$ is negligible and can be discarded. If $k \geq n$, one must make a verification query to eliminate false positives.
End Secret Info...

2. **(20 points)**[1] Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and consider the following variant of the $\mathsf{OCB2}$ mode of operation, which we call $\overline{\mathsf{OCB2}}$. For simplicity, we assume that associated data is always empty, hence it will be omitted from this exercise. $\overline{\mathsf{OCB2}}$ now operates as follows:

- Firstly, $\overline{\mathsf{OCB2}}$ takes a k-bit key K, n-bit nonce N, and arbitrary length message M. The message is split into blocks $M_1, M_2, \ldots, M_d$, where $M_1, \ldots, M_{d-1}$ are all of size n bits, and M_d is of size between 1 and n bits. A subkey $L = E_K(N)$ is computed.
- Secondly, $\overline{\mathsf{OCB2}}$ proceeds as in the picture:



[1]This exercise is based on an attack against OCB2 of Inoue et al.: `https://eprint.iacr.org/2019/311.pdf`.



Here, $\mathsf{len}(X)$ denotes the length of a bit string X, $\langle n \rangle$ is the binary representation of n, and $\ominus\!\leftarrow \mathrm{msb}_l$ denotes the truncation to the l most significant bits, i.e., the dropping of the right $n - l$ bits.

- Thirdly, it outputs ciphertext $C = C_1 \| C_2 \| \cdots \| C_d$ and tag T.

(a) Describe how the verification function of $\overline{\mathsf{OCB2}}$ works. I.e., given a k-bit key K, n-bit nonce N, arbitrary length ciphertext C, and an n-bit tag T, describe:

   i. How to determine if the tag is valid.

   ii. How to recover the plaintext M, if (N, A, C, T) is a correct authenticated ciphertext.

(b) It turns out that this version of $\overline{\mathsf{OCB2}}$ is, in fact, not secure. Consider an adversary that does the following:

   - Let N be an arbitrary nonce, and let $M = M_1 \| M_2$ be a $2n$-bit message with $M_1 = \langle n \rangle$ and M_2 any n-bit string.
   - The adversary calls the encryption oracle with input $(N, M_1 \| M_2)$, and obtains $(C_1 \| C_2, T)$.
   - The adversary takes a ciphertext $C' = C_1 \oplus \langle n \rangle$ of length n bits, and tag $T' = M_2 \oplus C_2$.
   - The adversary outputs forgery (N, C', T').

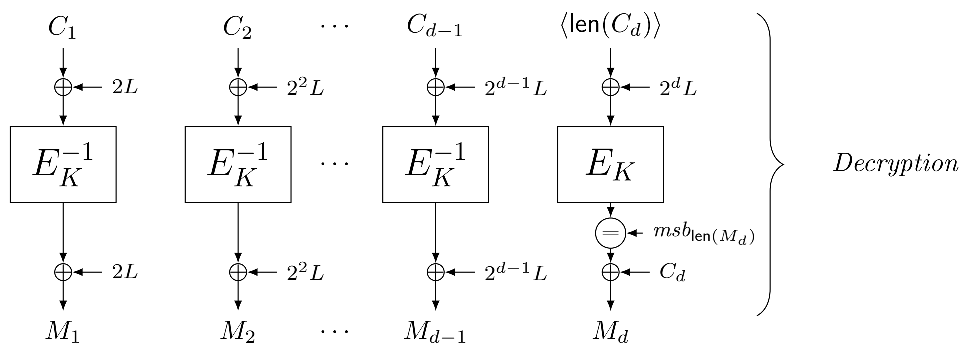
   Show that this forgery is valid. In order to do this, we recommend to proceed as follows:

   i. Compute M', the plaintext corresponding to C'.

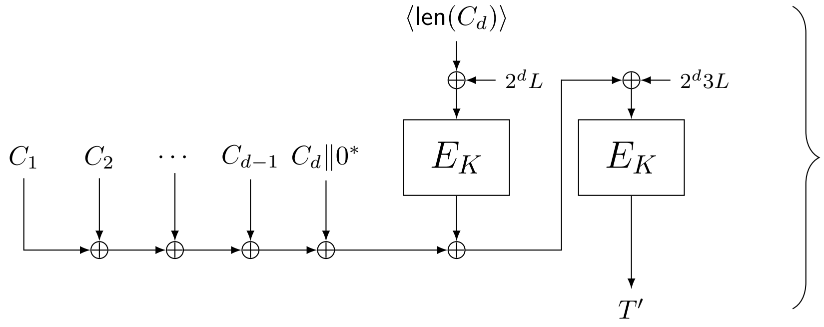
   ii. Compute $\overline{\mathsf{OCB2}}(N, M')$. **Hint**: Here, you need to use that in a binary field we have $2 \cdot 3 \oplus 2 = 2^2$.

Begin Secret Info: . . . .

(a) Note that M_d and C_d have the same length, hence $\langle n \rangle$ can be recovered as the length of C_d. So for decryption we proceed as follows:



***Note**: The last E_K is <u>not</u> a typo.*
As for verification, we only need recompute the tag, in the same way:



And then check whether $T \stackrel{?}{=} T'$.

(b) *Take* $T' = M_2 \oplus C_2$. *We have the following information:*

i. $M = M_1 \| M_2, \quad M_1 = \langle n \rangle$

ii. $\mathsf{len}(M_2) = n$.

iii. *We are also given:* $C' = C_1 \oplus \langle n \rangle$.

Hence, we can compute:

i. $C_1 = 2L \oplus E_K(2L \oplus \langle n \rangle)$.

ii. $C_2 = M_2 \oplus E_K(2^2L \oplus \langle n \rangle)$.

So if we try to decrypt C' *we get:*

$$M' = C' \oplus E_K(2L \oplus \langle n \rangle) = C_1 \oplus \langle n \rangle \oplus E_K(2L \oplus \langle n \rangle) = 2L \oplus E_K(2L \oplus M_1) \oplus \langle n \rangle \oplus E_K(2L \oplus \langle n \rangle) = 2L \oplus \langle n \rangle \,. \tag{1}$$

From this, we can recompute the tag:

$$T' = E_K(C' \oplus 2 \cdot 3L \oplus E_K(2L \oplus \langle n \rangle)) = E_K(2L \oplus E_K(2L \oplus \langle n \rangle) \oplus \langle n \rangle \oplus 2 \cdot 3L \oplus E_K(2L \oplus \langle n \rangle))$$
$$= E_K(2L \oplus 2 \cdot 3L \oplus \langle n \rangle) \stackrel{2\cdot 3 \oplus 2 = 2\cdot 2 \oplus 2 \oplus 2 = 2^2}{=} = E_K(2^2L \oplus \langle n \rangle) = M_2 \oplus C_2.$$

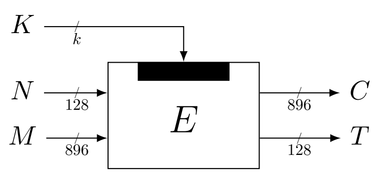
So (N, C', T') *is a valid forgery.*

End Secret Info ....

3. **(10 points)** Consider a block cipher $E : \{0,1\}^k \times \{0,1\}^{1024} \to \{0,1\}^{1024}$ and consider the following authenticated encryption scheme

$$\begin{aligned} \mathsf{AE}\colon \{0,1\}^k \times \{0,1\}^{128} \times \{0,1\}^{896} &\to \{0,1\}^{896} \times \{0,1\}^{128}\,, \\ (K, N, M) &\mapsto (C, T)\,, \end{aligned}$$

defined as follows:



We will consider the nonce-misuse-resistance of this scheme. In other words, we consider the security of this construction in the model of lecture 3 slide 4, $\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{AE}}(q_e, q_v)$, *with the difference that $\mathcal{D}$ may repeat nonces.* Here, q_e and q_v denote the total number of encryption and decryption queries, respectively.

(a) Describe how the authenticated decryption function AE_K^{-1} operates.

(b) The first step in the security proof of AE will be to replace the keyed block cipher E_K by a random permutation p. Apply the triangle inequality to do so, with explicitly mentioning the loss incurred by this triangle inequality:

$$\Delta_{\mathcal{D}}\left(\mathsf{AE}_K, \mathsf{AE}_K^{-1} \ ; \ \$, \perp\right) \leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \$, \perp\right) + \dots$$

Explain your answer in words.

(c) We are left with the task of bounding $\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \$, \perp\right)$. We will perform another triangle inequality:

$$\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \$, \perp\right) \leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \mathsf{AE}[p], \perp\right) + \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \perp \ ; \ \$, \perp\right) . \tag{2}$$

The first distance of (2) is a bit peculiar and will be ignored in this assignment. Derive a bound on the second distance of (2), $\Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \perp \ ; \ \$, \perp\right)$.

Begin Secret Info:. . . . .

(a) AE_K^{-1} gets as input a tuple (N, C, T). It evaluates $E_K^{-1}(C, T)$ and parses the outcome as $M \| N^*$. If $N = N^*$ it outputs M, otherwise it outputs $\perp$.

(b) As in the lectures:

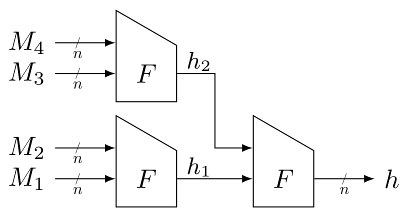
$$\begin{aligned}\Delta_{\mathcal{D}}\left(\mathsf{AE}_K, \mathsf{AE}_K^{-1} \ ; \ \$, \perp\right) &\leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \$, \perp\right) + \Delta_{\mathcal{D}}\left(\mathsf{AE}_K, \mathsf{AE}_K^{-1} \ ; \ \mathsf{AE}[p], \mathsf{AE}[p]^{-1}\right) \\ &\leq \Delta_{\mathcal{D}}\left(\mathsf{AE}[p], \mathsf{AE}[p]^{-1} \ ; \ \$, \perp\right) + \mathbf{Adv}^{\mathrm{sprp}}_{E}(q_e + q_v) .\end{aligned}$$

Here, it is important to note that we take SPRP security and not PRP security as the adversary can technically trigger inverse evaluations of E.

(c) Note that the decryption oracle is redundant, and we have to basically consider the PRF-security of $\mathsf{AE}[p]$ under q_e encryption queries. First apply the RP-to-RF-switch (i.e., replace p by f) at the cost of $\binom{q_e}{2}/2^{1024}$. Then, any response is uniformly randomly distributed from $\{0,1\}^{1024}$ and the worlds are indistinguishable.

End Secret Info . . . .

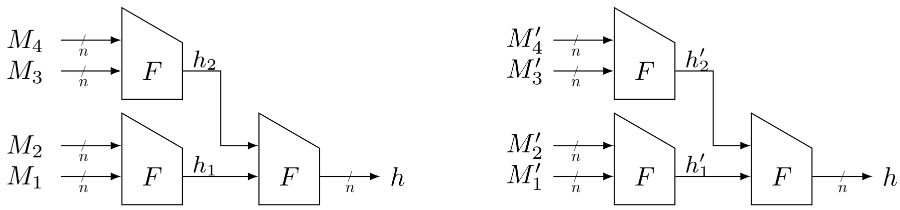
4. **(10 points)** We will cover the Merkle-Damgård and other *sequential* hashing modes in lecture 4, and this question is an introductory teaser towards this lecture.. An alternative to sequential hashing is tree-based hashing. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a compression function, and consider the following hash function $\mathcal{H} : \{0,1\}^{4n} \to \{0,1\}^n$:



Argue (informally) that $\mathcal{H}$ is collision resistant if F is collision resistant.

Begin Secret Info:..

Suppose we find two different messages (M_1, M_2, M_3, M_4) *and* (M'_1, M'_2, M'_3, M'_4) *that yield the same hash:*



- *Clearly, if* $h_1 \neq h'_1$ *or* $h_2 \neq h'_2$*, then* $F(h_1, h_2) = h = F(h'_1, h'_2)$ *forms a non-trivial collision for* F*.*
- *Otherwise, if both* $h_1 = h'_1$ *and* $h_2 = h'_2$*, we distinguish between two cases:*
  - $(M_1, M_2) \neq (M'_1, M'_2)$*: then* $F(M_1, M_2) = h_1 = F(M'_1, M'_2)$ *forms a non-trivial collision for* F*.*
  - $(M_3, M_4) \neq (M'_3, M'_4)$*: then* $F(M_3, M_4) = h_2 = F(M'_3, M'_4)$ *forms a non-trivial collision for* F*.*

End Secret Info..