CS 578 – Cryptography (Summer 2006) Prof. Michael Backes

Mid-term Exam

Date: 05/30/2006 Saarland University

Name Matriculation

- **DO NOT OPEN** this exam until instructed to do so. Read all the instructions first.
- When the exam begins, first write your name on every page of this exam.
- This exam contains 5 pages including this one. Two extra sheets of scratch paper are attached.
- This exam is closed-book, closed-notes.
- The exam offers you four problems to solve. **Pick three out of four that you would like to solve**. You have to clearly mark down on this page which of these four problems should count for your grade. This means that solving all four problems will not give you any bonus, since you have to identify which three problems should count!
- You have 1 hour for the exam. Every problem gives 20 points. Since you have to pick three out of four problems, there are 60 points to achieve.
- Write your solutions in the space provided. In case you need extra space, write on the back of the sheet containing the question. Do not put part of the answer to one problem on the back of the sheet for another problem; pages may be separated for grading.
- **Be neat and write legibly**. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it. In particular, if you are asked to show (both prove or disprove) a statement, the closer you can come to a (correct) formal statement the better.
- Good luck!

At the end of the exam, circle which problems you'd like to see graded (**at most three out of four**):

Problem 1 **Problem 2** **Problem 3** **Problem 4**

Name Matriculation

Problem 1: True or False? (20 Points)

Circle true or false for each of the following statements. No justification is required, but if you think that the question is ambiguous, state your clarifying assumptions on the back of this page. **Each correct answer gives two points, each wrong answer deduces two points**. An overall negative score for this problem is not possible.

true	false	Using a one-time pad for encryption, followed by a CBC-MAC (using a PRP) on the resulting ciphertext, provides perfect secrecy and security against existential forgeries under CMA.
true	false	Given an AES key K, it is possible to efficiently construct a one-kilobyte plaintext message m such that an encryption of m under AES (using key K) in deterministic countermode consists only of 0's.
true	false	The design of a Feistel network requires that the round functions f_i, i.e., the functions such that $R_i = L_{i-1} \oplus f_i(R_{i-1})$, be invertible.
true	false	If $\mathsf{H}(\cdot)$ is a collision-resistant hash function, then $\mathsf{H}(\mathsf{H}(\cdot))$ is also a collision-resistant hash function.
true	false	If (as conjectured) SHA-256 is collision-resistant, then there are no two distinct inputs that hash to the same value.
true	false	SHA-1 with its digests of 160 bits is more resistant to attacks based on the birthday paradox than MD5 with its digests of 128 bits.
true	false	There are deterministic encryption schemes that are semantically secure under ciphertext-only attack.
true	false	The function $h(k) = (\frac{1}{2})^{\sqrt{k}}$ is negligible.
true	false	The function $h(k) = \frac{x^k}{(x^y)^k}$ is negligible for all fixed natural numbers x, y satisfying $x > 1$ and $y > 1$.
true	false	Moore's Law says that the speed of computers doubles every 18 months. Consequently, one should update one's secret keys at least once every 18 months.

Problem 2: A Variant of MAC Security (20 Points)

In class we introduced the notion that a MAC is secure against existential forgery under a chosen-message attack (CMA), i.e., the adversary gets tags for arbitrary messages of its choice and has to subsequently produce an existential forgery. This is depicted again in Figure 1.

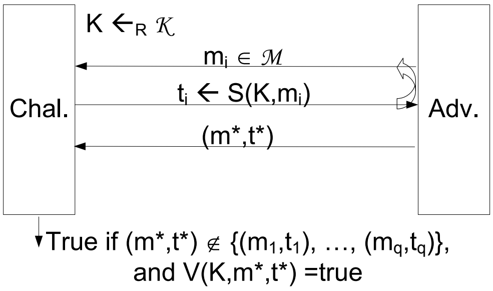


Figure 1: CMA-Game for a MAC (S, V) over $(\mathcal{K}, \mathcal{M}, \mathcal{T})$

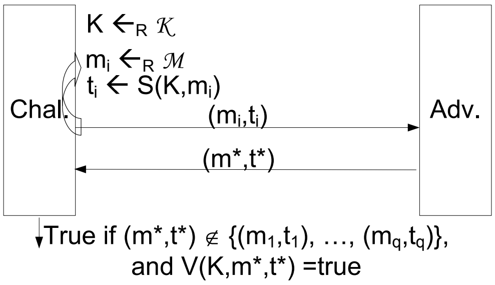


Figure 2: RMA-Game for a MAC (S, V) over $(\mathcal{K}, \mathcal{M}, \mathcal{T})$

Consider the following variant of this definition: Assume that the challenger does not receive messages m_i from the adversary, but instead the challenger randomly chooses messages m_i, computes their tags t_i and outputs the pairs (m_i, t_i). A q-query adversary is given q of these pairs $(m_1, t_1), \ldots, (m_q, t_q)$ (where the messages m_i have been chosen randomly and independent of each other) and has to produce a valid forgery as usual. We say that a MACs is secure against existential forgery under a *random* message attack (RMA), if the advantage of every efficient q-query adversary is negligible in this game (for q being any polynomial). This is shown in Figure 2.

Clearly MACs that are secure under CMA are also secure under RMA. Show that the converse is false, i.e., show that there exists an RMA-secure MAC that is not CMA-secure.

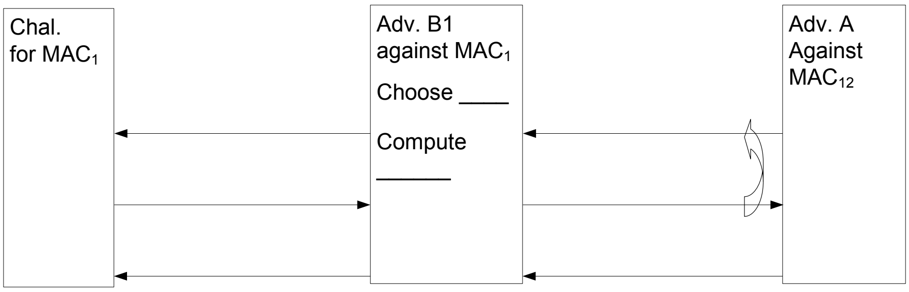
Hint: Suppose (S, V) is a CMA-secure MAC. Slightly change this MAC into a new MAC $(\mathsf{S}^*, \mathsf{V}^*)$ that is still RMA-secure but that is obviously insecure under CMA.

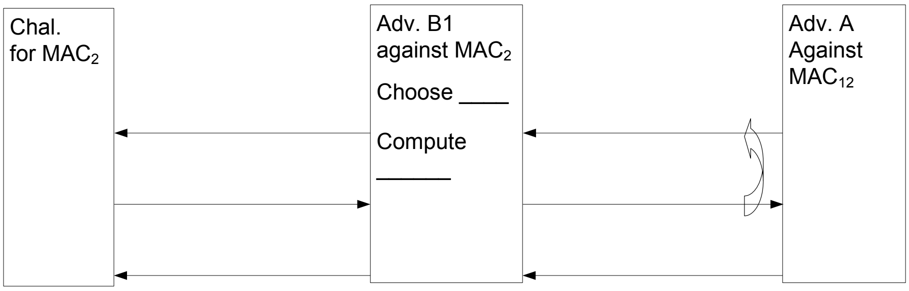
Name Matriculation

Problem 3: Strengthening Hashes (10 + 10 Points)

(a) Suppose we are given two hash functions $\mathsf{H}_1, \mathsf{H}_2 \colon \{0,1\}^* \to \{0,1\}^n$ and are told that both hash functions are collision-resistant. We, however, do not quite trust these claims. Our goal is to build a hash function $\mathsf{H}_{12} \colon \{0,1\}^* \to \{0,1\}^m$ (for some m) that is collision-resistant assuming *at least one* of H_1, H_2 is collision-resistant. Give a construction for H_{12} and prove that an adversary that finds collision for your H_{12} can be used to find collisions for both H_1 and H_2 (this will prove collision resistance of H_{12} assuming one of H_1 or H_2 is collision-resistant). Note that a straightforward construction for H_{12} is fine, as long as you can prove that your construction finds collisions for both H_1 and H_2 if given an adversary that finds collisions for H_{12}.

(b) Same questions as in part (a) for Message Authentication Codes (MACs): Given two MACs MAC_1, MAC_2, construct a MAC MAC_{12} that is CMA-secure assuming that at least one of MAC_1 and MAC_2 is CMA-secure. Show that an adversary A that breaks the CMA-security of MAC_{12} can be used to find two adversaries B_1 and B_2 that break the CMA-security of MAC_1 and MAC_2, respectively. Again, a straightforward construction is fine. The proof of security here is a bit more involved than in part (a); thus it suffices to construct the adversaries $\mathsf{B}_1, \mathsf{B}_2$ by completing the figures below. No additional proof has to be given.



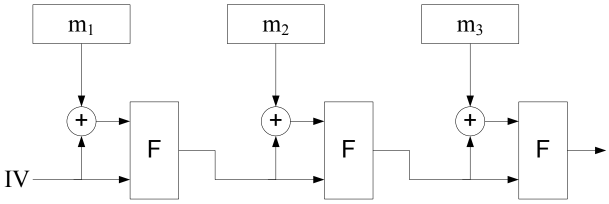


Name Matriculation

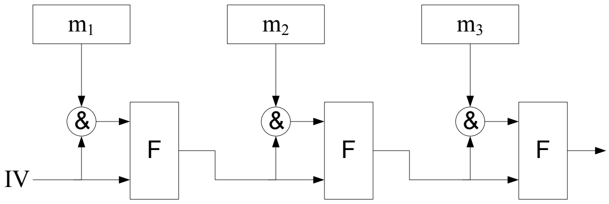
Problem 4: Modified Merkle-Damgard Construction (20 Points)

One might try to modify the Merkle-Damgard construction for hash functions in the following three ways. One of the three constructions is a collision-resistant hash function, while the other two constructions are not.

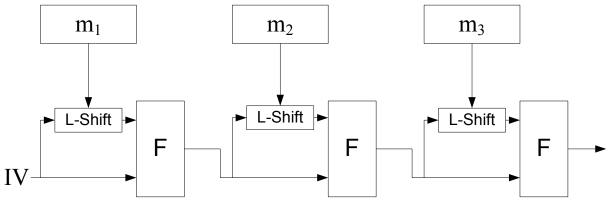
Construction 1:



Construction 2:



Construction 3:



In Construction 1, + is a bit-wise XOR. In Construction 2, & is a bit-wise AND-operation. In Construction 3, L-Shift cyclically shifts the chaining-variable to the left by m_i positions, where the bitstring m_i is interpreted as the corresponding natural number.

The initial vector IV = 5c5c...5c is public in all constructions. Suppose F is a collision-resistant compression function that takes a 512 bit message block and a 512 bit chaining value, and outputs a 512 bit result. Answer **one of the following two** questions; **clearly mark which one you chose.**

(a) Show how to construct collisions for the two constructions that are not collision-resistant,
–or–
(a') Prove that the remaining construction is collision-resistant.

Name	Matriculation

Name Matriculation