Preamble

This sheet is split into two parts. Problems 1-2 may be attempted after the lesson of Thursday 25/10/2018 and problems 3-6 should be attempted after the lesson of Monday 29/10/2018.

Questions

Problem 1

Prove that the following modifications of CBC-MAC do not yield a secure fixed-length MAC:

(a) Modify CBC-MAC so that a random IV is used each time a tag is computed (and the IV is output along with t_l). I.e., $t_0 \leftarrow \{0,1\}^n$ is chosen uniformly at random rather than being fixed to 0^n, and the tag is (t_0, t_l).

(b) Modify CBC-MAC so that all blocks $t_1, \ldots, t_l$ are output (rather than just t_l).

Problem 2

In this question we define basic notation required for protocol exchange and ask you what vulnerabilities several protocols may possess. We define the following notation.

- We let A, B denote Alice and Bob respectively.
- We let C denote a trusted third-party server, who adheres honestly to the protocol.
- Let Id_A, Id_B, Id_C, Id_E, also denote the publicly known identities of Alice, Bob, the trusted third-party server and Eve, respectively.
- We let E denote Eve, an adversary who has the power to passively eavesdrop, modify, block, store or entirely replace any transmission they perceive.
- We let N_i (for $i \in \mathbb{N}$) denote a *Nonce*, or a randomly sampled number used only once. Any party may create any number of nonces.
- $\{m\}_{k(X,Y)}$ denotes that the message m has been encrypted with a symmetric key k shared by X and Y. m may be recursively defined as $m = m', m''$ or $m = \{m'\}_k$ or $m = Id_x$ or $m = N_i$.
- n. $X :\longrightarrow Y :$ m is interpreted as "In step n, X sends Y the message m".

Alice and Bob live in an almost perfect world, where they have unbreakable symmetric-key encryption. This world (much like yourselves in the course) has not yet seen the introduction of public-key cryptography. The only thing that they both know is the public identity of each other and that C is a trusted third-party server, with whom they share the keys with (A and C both possess knowledge of $k(A,C)$ whilst B and C both possess knowledge of $k(B,C)$).

In protocol 1) Alice and Bob seek to establish a shared secret key $k(A,B)$.
In protocol 2), Bob seeks to confirm that he is communicating with Alice.

Can the protocols be subverted by Eve?

Protocol 1: Key Establishment

1. $A \longrightarrow B :$ $Id_A, \{Id_A, N_a\}_{k(A,C)}$
2. $B \longrightarrow C :$ $Id_B, \{Id_A, \{Id_A, N_a\}_{k(A,C)}\}_{k(B,C)}$
3. $C \longrightarrow B :$ $Id_C, \{Id_A, N_a\}_{k(B,C)}$
4. $k(A,B) := N_a$

Protocol 2: Identity establishment

1. $A \longrightarrow B :$ Id_A
2. $B \longrightarrow A :$ N_b
3. $A \longrightarrow B :$ $\{N_b\}_{k(A,C)}$
4. $B \longrightarrow C :$ $\{A, \{N_b\}_{k(A,C)}\}_{k(B,C)}$
5. $C \longrightarrow B :$ $\{N_b\}_{k(B,C)}$

Problem 3

Let (Gen_1, H_1), (Gen_2, H_2) be two hash functions. Define (Gen, H) so that Gen runs Gen_1 and Gen_2 to obtain keys s_1 and s_2, respectively.
Then define $H^{s_1,s_2}(x) := H_1^{s_1}(x)||H_2^{s_2}(x)$.

(a) Prove that if at least one of (Gen_1, H_1) and (Gen_2, H_2) is collision resistant, then (Gen, H) is collision resistant.

(b) Is (Gen, H) pre-image resistant if at least one of (Gen_1, H_1) and (Gen_2, H_2) is pre-image resistant?

Problem 4

The definition of collision-resistance for hash-functions was provided to you in the lectures:

Definition (Collision-resistant hash-function)
A hash-function $\Pi = (\mathsf{Gen}, H)$ *is* collision resistant *if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that the success probability of* $\mathcal{A}$ *winning the* $\mathsf{Hash\text{-}coll}_{\mathcal{A},\Pi}(n)$ *experiment defined below is negligible.*

The collision-finding experiment $\mathsf{Hash\text{-}coll}_{\mathcal{A},\Pi}(n)$**:**

1. *A key* $s \leftarrow \mathsf{Gen}(1^n)$ *is generated.*
2. *The adversary* $\mathcal{A}$ *is given* s *and outputs* $x, x' \in \{0,1\}^*$ *(the length is restricted to* $x, x' \in \{0,1\}^{l(n)}$ *if* Π *is a fixed length hash-function).*
3. *The output of the experiment is defined to be 1 if and only if* $x \neq x'$ *and* $H^s(x) = H^s(x')$*. In this case we say that* $\mathcal{A}$ *has found a collision.*

Create a formal definition for *second-preimage resistance* as given in the lectures and prove that a collision-resistant hash-function is also second-preimage resistant.

Problem 5

Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) := H^s(H^s(x))$ necessarily collision resistant?

Problem 6

Before HMAC was invented, it was quite common to define a MAC by $\mathsf{Mac}_k(m) = H^s(k||m)$ where H is a collision-resistant hash-function. Show that this is not a secure MAC when H is constructed via the Merkle-Damgård transform.