Università degli Studi di Padova

# Information Security class
# written exam

Dipartimento di Ingegneria dell'Informazione

instructor: Nicola Laurenti

Academic year 2020-21

Summer session, second call    June 30, 2021

student name ______________________________ number ________________

## *Instructions for candidates*

*The maximum allowed time is 2 (two) hours, and students who complete their exam in less time can submit it and leave the room*

*The exam is* open book *and* open notes, *which means that you can make use of any textbook, lecture notes, literature papers, etc., you brought with you.*

*You are not, however, allowed to communicate with anyone, inside or outside the room, so the use of phones, tablets, computers is forbidden at any time during the exam. If you need a computing support, bring an old fashioned pocket calculator with you.*

*For the same reason, no exchange of material is allowed among students, and each student can only exit the room after completing his/her exam.*

*The result of this exam is given in the scale* ***excellent*** */* ***very good*** */* ***good*** */* ***fair pass*** */* ***pass*** */* ***fail****. All grades except* ***fail*** *grant admission to the final oral exam.*

## Problem 1

Consider a sequence of security mechanisms $M_n$, $n \in \mathbb{N}$ that have a deterministic running time $T_{M_n} = T_0(n^2 + n)$ with $T_0 = 1\,\text{ns}$, and a class $\mathcal{A}$ of attacks such that each attack $A_n \in \mathcal{A}$ against $M_n$ has success probabiity depending on its running time $T_{A_n}$ as follows

$$\mathrm{P}\left[S_{\mathcal{A}}; A_n, M_n\right] = \begin{cases} \dfrac{T_{A_n}}{2^n T_{M_n}} & , \text{ if } 0 \leq T_{A_n} < 2^n T_{M_n} \\ 1 & , \text{ otherwise} \end{cases}$$

1.1) Compute an upper bound to the probability that an attack from $\mathcal{A}$ against $M_{100}$ succeeds within $T_1 = 1\,\text{year}$

1.2) Is the sequence of mechanisms $M_n$ computationally secure in the asymptotic sense against the attack class $\mathcal{A}$? Justify your answer

$h(k) \geq \lfloor \log_{1/2} \varepsilon \rightarrow \geq \underbrace{\lceil 2 \cdot \log_{1/2} 10^{-6} \rceil} = 39{,}86. \simeq 40 \rightarrow H(k)=40$

$I(k,x) \leq \min\{\underset{40}{\underset{\vee\!\mid}{H(k)}}, \underset{\geq 40}{\underset{\vee\!\mid}{H(x)}}\}$

## Problem 2

In a cryptographic mechanism for message authentication and integrity protection, the mutual information between the key $k$ and the signed message $x$ is $I(k, x) = 40\,\text{bit}$

2.1) Find the minimum entropy of the key that is necessary so that any illegitimate modification attack succeeds with probability below $10^{-6}$, while all unmodified messages are accepted. Is the above condition on the key entropy also sufficient to this aim?

9

2.2) Prove that there exists a forgery threat against which no verification rule can achieve false alarm and missed detection probabilities $p_{\text{FA}}$ and $p_{\text{MD}}$, resepctively, such that $p_{\text{FA}} \leq 10^{-3}$ and $p_{\text{MD}} \leq 10^{-13}$

$\log_{1/2} 10^{-13} \rightarrow 43.$

$\frac{1}{10^6}$

$43 > 40.$

## Problem 3

Consider the following protocol, by which an entity A wants to establish secret communication with another entity B

**entities** the initiator A, the target entity B, a trusted third party C

**tools** an asymmetric encryption mechanism $(E'_{k'}(\cdot), D'_{k}(\cdot))$ between C and A, and between C and B;
a symmetric encryption mechanism $(E_k(\cdot), D_k(\cdot))$ between A and B;
a (deterministic) cryptographic hash function $h(\cdot)$

**setup** C knows the public keys $k'_{\mathsf{A}}, k'_{\mathsf{B}}$ of A and B, respectively, for the asymmetric encryption

$\boxed{1}$ A : generates a nonce $n_{\mathsf{A}}$
A → C : $u_1 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}})$ $\longrightarrow$ E.

$\boxed{2}$ C : C generates $k_{\mathrm{AB}} \sim \mathcal{U}(\mathcal{K})$
builds message $u_2 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}}, k_{\mathrm{AB}})$
computes its hash $v_2 = h(u_2)$
encrypts their concatenation $x_2 = E'_{k'_{\mathsf{A}}}(u_2, v_2)$
C → A : $x_2$

PROBLEMA :

C non è sicuro

$\boxed{3}$ A : decrypts $(u_2, v_2) = D'_{k_{\mathsf{A}}}(x_2)$
verifies that $v_2 = h(u_2)$
checks that $\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}}$ are correct

$\boxed{4}$ A → B : $u_1$

$\boxed{5}$ B : generates a nonce $n_{\mathsf{B}}$
B → C : $u_5 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}}, n_{\mathsf{B}})$

$\boxed{6}$ C : builds message $u_6 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}}, n_{\mathsf{B}}, k_{\mathrm{AB}})$
computes its hash $v_6 = h(u_6)$
encrypts their concatenation $x_6 = E'_{k'_{\mathsf{B}}}(u_6, v_6)$
C → B : $x_6$

$\boxed{7}$ B : decrypts $(u_6, v_6) = D'_{k_{\mathsf{B}}}(x_6)$
verifies that $v_6 = h(u_6)$
checks that $\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, n_{\mathsf{A}}, n_{\mathsf{B}}$ are correct

non è garantita integrità da parte C .

$\boxed{8}$ B → A : $u_5$

$\boxed{9}$ A and B start encypting their communications with $E_{k_{\mathsf{AB}}}$ and $D_{k_{\mathsf{AB}}}$

3.1) identify the protocol vulnerabilities and devise an attack that exploits them, under reasonable assumptions;

3.2) suggest limited changes and/or improvements to the protocol that can solve the above issues.