

Information Security class written exam



instructor: Nicola Laurenti

Academic year 2020-21 Fall session, second call September 10, 2021

4 1 4	1
student name	number

Instructions for candidates

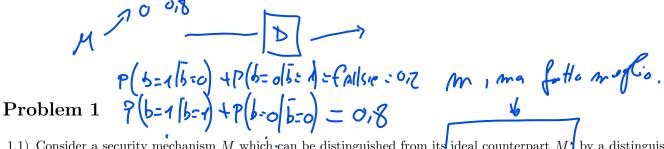
The maximum allowed time is 2 (two) hours, and students who complete their exam in less time can submit it and leave the room

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.



- 1.1) Consider a security mechanism M which can be distinguished from its ideal counterpart M^* by a distinguisher D with the following probabilities
 - D correctly identifies M with probability 0.8
 - D correctly identifies M^* with probability 0.25

Can you find an *upper bound* to the unconditional security level of M in terms of distinguishability? Can you find a *lower bound*?

- 1.2) Consider a sequence of security mechanisms M_n , $n=2,3,\ldots$ and their ideal counterparts M_n^{\star} . Suppose there exist a sequence of distinguishers D_n between M_n and M_n^{\star} such that
 - D_n runs in a deterministic time $T_{D_n} = (n^2 + 1)T_0$, where $T_0 = 1 \,\mu\text{s}$
 - D_n correctly identifies M_n with probability $1/n + 1/2^n$
 - D_n correctly identifies M_n^{\star} with probability $(n-1)/n + 1/2^n$

Can you state that the sequence of mechanisms M_n is computationally secure in the asymptotic sense? Justify your answer

Problem 2

Consider a discrete time wiretap AWGN channel in which

- the symbol time is $T = 10 \,\mu s$
- the legitimate channel has an amplitude gain g = 1/100 and a noise variance $\sigma_w^2 = 10^{-6} \, \mathrm{V}^2$
- the eavesdropper channel has an amplitude gain h = 1/200 and a noise variance $\sigma_n^2 = 2 \cdot 10^{-6} \, \text{V}^2$
- 2.1) Find the minimum time interval that is necessary to transmit a secret message of $\ell = 100\,\mathrm{kbit}$ over this wiretap channel with arbitrary transmit power.
- 2.2) Find the minimum statistical power of the transmitted symbols that is necessary to transmit the same message over a time interval of $T_1 = 1 \,\mathrm{s}$

Problem 3

Consider the following entity authentication protocol, by which A wants to prove itself to B

entities the prover A, the verifier B

tools a large prime integer N, a number $g \in \{2, ..., N-1\}$, both publicly known an identifier id_A , and a secret key $k_A \in \{2, ..., N-1\}$

setup A securely shares its credentials (id_A, k_A) with B, who stores them in a secure database.

- $1 \land A \rightarrow B : x_1 = (id_A, id_B)$
- 2 B: generates a random challenge $c \sim \mathcal{U}(\mathbb{Z}_N)$ B \rightarrow A: $x_2 = c$
- $\begin{tabular}{ll} \hline {\tt 3} & {\tt A}: \mbox{ computes response } r=g^{k_A+c} \mbox{ mod } N, \, r \in \mathbb{Z}_N \\ & {\tt A} \rightarrow {\tt B}: \ x_3=(\mathrm{id}_A,c,r) \\ \end{tabular}$
- 4 B: looks up k_A and computes expected response $\hat{r} = g^{k_A + c} \mod N$ if $\hat{r} = r$, A is accepted as authentic, otherwise rejected
- 3.1) identify the protocol vulnerabilities against a dishonest prover F who aims to pose as A and devise an attack by F that exploits them, under reasonable assumptions;
- 3.2) suggest limited changes and/or improvements to the protocol that can solve the above issues;
- 3.3) suggest limited changes and/or improvements to the protocol that can introduce non transferability agains a dishonest verifier B who aims to later pose as A towards another verifier C;

student name number



