UNIVERSITÀ DEGLI STUDI DI PADOVA

Information Security class written exam

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

instructor: Nicola Laurenti

Academic year 2020-21
Winter session, second call   February 13, 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, have with you an old fashioned pocket calculator.

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

Given a binary string $a \in \{0,1\}^n$ let $\bar{a}$ denote its *bitwise complementary*, that is

$$\bar{a} = a \oplus [1, 1, \ldots, 1]$$

Consider a cryptographic hash function $h : \{0,1\}^\ell \mapsto \{0,1\}^n$, and by modeling it as an ideal random function,

1.1) prove that the probability of finding at least one pair of complementary hash outputs among L distinct input strings is the same as that of finding at least one pair of colliding hash outputs

1.2) compute upper and lower bounds to the above probability for $\ell = 1024$, $n = 100$, $L = 10^{15}$

1.3) assuming a single hash can be computed in $T_\mathrm{h} = 10\,\mu\mathrm{s}$ and neglecting all other computation (e.g., sorting, comparing) times, state whether the hashing function h with $\ell = 1024$, $n = 100$, is (ε, T_0) computationally secure against collision attacks, with $\varepsilon = 10^{-6}$ and $T_0 = 1\,\mathrm{year}$

Problem 2

A true random number generator outputs binary independent and non uniform symbols $\{z_n\}$ with distribution $p_z(0) = 51\%$, $p_z(1) = 49\%$

2.1) Prove that a sequence of $N = 10$ symbols from the generator is ε-unconditionally secure for $\varepsilon = 0.04$

2.2) Assume the sequence is used as a one-time-pad encryption key for a 10-bit message, where 5 uniformly distributed bits are repeated twice, and compute an upper bound to the success probability of a guessing attack on the message

Problem 3

Consider the following protocol based on asymmetric cryptography by which two parties A and B aim at learning each other's public key

entities two legitimate parties A, and B, a trusted third party C

tools an Elgamal digital signature mechanism $(S_k(\cdot), V'_{k'}(\cdot))$ and an Elgamal encryption mechanism $(E'_{k'}(\cdot), D_k(\cdot))$

setup assume that private keys are only known to their corresponding entities, while public keys are known as follows:

- k'_{C} is known to both A and B;
- k'_{A} is known to C, but not to B;
- k'_{B} is known to C, but not to A.

$\boxed{1}$ $\mathsf{A}:$ generates nonce $r_{\mathrm{A}} \sim \mathcal{U}(\mathcal{R})$

$\mathsf{A} \to \mathsf{C}:$ $u_1 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, r_{\mathrm{A}})$

$\boxed{2}$ $\mathsf{C}:$ builds message $u_2 = (\mathrm{id}_{\mathrm{B}}, k'_{\mathrm{B}})$
signs it $x_2 = S_{k_{\mathrm{C}}}(u_2)$, using r_{A} as the random exponent in the first component of the Elgamal signature

$\mathsf{C} \to \mathsf{A}:$ x_2

$\boxed{3}$ $\mathsf{A}:$ retrieves and verifies $(u_2, \hat{b}_2) = V'_{k'_{\mathrm{C}}}(x_2)$
builds message $u_3 = (r_{\mathrm{A}}, \mathrm{id}_{\mathrm{A}})$ encrypts $x_3 = E'_{k'_{\mathrm{B}}}(u_3)$, using r_{A} as the random exponent in the first component of the ciphertext

$\mathsf{A} \to \mathsf{B}:$ x_3

$\boxed{4}$ $\mathsf{B}:$ $u_3 = D_{k_{\mathrm{B}}}(x_3)$
generates nonce $r_{\mathrm{B}} \sim \mathcal{U}(\mathcal{R})$

$\mathsf{B} \to \mathsf{C}:$ $u_4 = (\mathrm{id}_{\mathrm{A}}, \mathrm{id}_{\mathrm{B}}, r_{\mathrm{B}})$

$\boxed{5}$ $\mathsf{C}:$ builds message $u_2 = (\mathrm{id}_{\mathrm{A}}, k'_{\mathrm{A}})$
signs $x_5 = S_{k_{\mathrm{C}}}(u_5)$, using r_{B} as the random exponent in the first component of the Elgamal signature

$\mathsf{C} \to \mathsf{B}:$ x_5

$\boxed{6}$ $\mathsf{B}:$ retrieves and verifies $(u_5, \hat{b}_5) = V'_{k'_{\mathrm{C}}}(x_5)$

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

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

1

1.1 1 input

$$P(\text{coll}) = \frac{1}{2^{n-\ell}} = p(\text{compl})$$

1.2 <u>upper, lower bounds?</u>

with L inputs

$$P(\text{coll}) = \sum_{k=2}^{L} \binom{k}{L}\left(\frac{1}{2^{\ell-n}}\right)^{k} \cdot \left(1-\frac{1}{2^{\ell-n}}\right)^{L-k} =$$

$$= 1-\left[\left(1-\frac{1}{2^{\ell-n}}\right)^{L} + L\left(\frac{1}{2^{\ell-n}}\right)\left(1-\frac{1}{2^{\ell-n}}\right)^{L-1}\right]$$

1.3

$$L = \frac{T_o}{T_h} = 3{,}1536 \times 10^{12}$$

$$2^{1024} \to 2^{100} \qquad \frac{2^{1024}}{2^{100}} = 2^{924} \qquad \ell - n = 924$$

$2^{\ell-n}$ = number of inputs that have the same hash

2

2.1

$$P[S_A|AM] < \varepsilon \qquad X = [E_1 \dots E_{10}] \qquad E_1 = \begin{cases} 1 & p = 0{,}49 \\ 0 & p = 0{,}51 \end{cases}$$

best guess is all zeros

$$P[000..0] = \underset{0{,}0012}{(0{,}51)^{10}} < 0{,}01$$

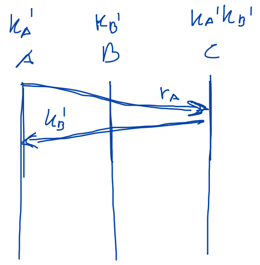
<u>yes</u>

2.2 $(m_S\, m_S) \oplus z_{10}$ first s bits of z_{10} determine the other five since

$$P\left(\begin{matrix}\text{most prob}\\ \text{guess}\end{matrix}\right) = (0{,}51)^{5} = 0{,}34 \qquad z_{[:5]} \oplus m_s = z_{[5:]} \oplus m_s$$

3

3.1 an evesdropper can learn r_A and x_2 and calculate k_C and then masquerade as C



public

id_a id_b r_A K_C'

K_B'

3.2 don't send r_A / r_B in plaintext but leave their choice to C