INL1Quiz Cryptographic Concepts 2023

Started: 21 Feb at 20:24

Quiz instructions

INL1 has 3 parts:

1. **INL1Quiz, a P/F quiz on canvas shortly after the lectures covering cryptography itself (Douglas's, Daniel's, and Roberto's lectures and Mats's lecture on randomness), about the material covered until then. The quiz will not monitored and is to be done individually without coordination with others. The quiz will be available for a week and you can take it according at your convenience during that time without time restriction.**
2. INL1Written, graded P/F, toward the end of the course, where you get to apply your knowledge. You will have a week to work on your solution (the task itself will take about half a day or a day at most.)
3. INL1Oral, graded P/F, at the end of the course (you'll pick one of the offered times and sign up), where you get about 10 minutes to answer some questions about your solution. There you can also clarify anything we found unclear in INL1Written, thus potentially getting the preliminary grade from that part improved.

Question 1

1 pts

Ciphers. Consider a cipher such that for each secret key $k \in \{0,1\}^n$ the resulting function E_k is a randomly chosen bijection $E_k : \{0,1\}^n \longrightarrow \{0,1\}^n$. Can such a cipher be implemented efficiently in a real-world application, i.e., in time and space polynomial in n?

● No

○ Yes

Question 2

1 pts

Ciphers. A substitution cipher is a function $E_k : L \longrightarrow S$ that for each secret key k and a letter from an alphabet L of constant size outputs a ciphertext symbol from a ciphertext alphabet S of constant size. A string is encrypted by encrypting each letter separately using the same key k.

Is it possible to construct a secure substitution cipher?

○ No

○ Yes

● Sometimes

Question 3

1 pts

Pseudo-randomness. Suppose that $PRG : \{0,1\}^n \longrightarrow \{0,1\}^{p(n)}$ be a pseudo-random generator that expands an n-bit string to a $p\left(n\right)$-bit string, where $p\left(n\right) > n$ is a polynomial. You work for a Casino and can either buy a hardware random device (blackbox) that produces true random bits, or you can sample a seed and use the pseudo-random generator to generate pseudo-randomness.

What is the advantage of using a pseudo-random generator in this application?

Edit View Insert Format Tools Table

12pt Paragraph

p

0 words

Question 4

1 pts

Pseudo randomness. Suppose that $PRG : \{0,1\}^n \longrightarrow \{0,1\}^{p(n)}$ is a pseudo-random generator that expands an n-bit string to a $p\left(n\right)$-bit string where $p\left(n\right) > n$ is a polynomial. We use it as follows. We sample a seed s and flip the first bit of s to form s'. Then we define $PRG'\left(s\right) = PRG\left(s\right) \mid PRG\left(s'\right)$. Is PRG' a pseudo-random generator?

● No

○ It depends on how PRG is defined.

○ Yes

Question 5

1 pts

Hash functions. Consider the Merkle-Damgård construction of a hash function $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ from a compression function $F : \{0,1\}^{2n} \longrightarrow \{0,1\}^n$. What happens if the padding block containing the length is removed?

○ The hash function is no longer one-way

● The hash function is no longer collision resistant

○ The hash function is both one way and collision resistant

Question 6

1 pts

Hash functions. Let $h : \{0,1\}^* \longrightarrow \{0,1\}^*$ be a one way function. Does this imply that it is collision resistant?

● No

○ Yes

Question 7

1 pts

Asymmetric cryptography.

When an electronic signature of a message claimed to be produced by Alice is verified we typically verify (at least the first time):

1. that the public key belongs to Alice by verifying that it has been signed (along with additional information) by a certificate authority (CA) who we trust (such a signature is called a "certificate"),
2. that the verification algorithm accepts the signature as valid for the message.

Suppose that you receive public keys pk_A, pk_X, and pk_Y and signatures s_A, s_X, and s_Y such that:

- $Vf_{pk_A}(s_A, m) = 1,$
- $Vf_{pk_X}(s_X, ”\ Alice's\ public\ key\ is\ pk_A\ ”) = 1$
- $Vf_{pk_Y}(s_Y, ”\ X's\ public\ key\ is\ pk_X\ ”) = 1$

where Vf denotes the verification algorithm of the signature scheme. You know that pk_Y belongs to the certificate authority Y. Is this is enough to be confident that Alice signed m?

○ yes

● no

Question 8

1 pts

Zero knowledge proofs. Match properties of zero knowledge proofs (of knowledge) with their informal definitions.

Completeness	A transcript of an interactic ⬍
Soundness	The verifier accepts a false ⬍

Knowledge extraction	The prover knows a specifi ⬍
Zero knowledge	When both parties are hon ⬍

Question 9

1 pts

Secure Multiparty Computation. Consider the protocol for Garbled circuits that we have seen during the lecture. Let Alice be the participant that encrypts the circuit and Bob be the participant that evaluates the circuit.

Let Alice be a malicious (active) adversary (i.e. she does not follow the protocol properly). Can she learn (violate confidentiality of) Bob's input? Motivate your answer, in general or with an example.

Edit View Insert Format Tools Table

12pt ⌄ Paragraph ⌄ | B *I* U A ⌄ ⌄ T² ⌄ | ⋮

p ⌨ 0 words | </> ⤢ ⠿

Question 10

1 pts

Secure Multiparty Computation. Consider the protocol for Garbled circuits that we have seen during the lecture. Let Alice be the participant that encrypts the circuit and Bob be the participant that runs the circuit.

Suppose that Alice and Bob want to compute the output of a function F for two pairs of inputs (i.e. a=F(x1, y1) and b=F(x2,y2), where Alice knows x1 and x2 and Bob knows y1 and y2. Suppose that Alice encrypts the circuit representing F once, that she sends the resulting garbled circuit to Bob, and that she allows Bob to obtain the encryption of both inputs y1 and y2, so that he can run the same circuit twice. Is this secure for Alice? Motivate your answer, in general or with an example.

Edit View Insert Format Tools Table

12pt Paragraph

p

0 words

Saved at 20:43

Submit quiz