Thema: Slides Required

erstellt von Muhammad Hassan am Freitag 09. November 2018, 16:02

Dear Prof.
Please upload the lecture slides.
Thanks

Thema: Optional Topic

erstellt von Muhammad Hassan am Sonntag 10. Februar 2019, 12:37

Hi,
can anyone tell me which topic is optional either Intro or differential privacy?
Thanks

---

erstellt von Korbinian Spielvogel am Sonntag 10. Februar 2019, 12:39

None of them is optional. Both are mandatory for the exam

---

erstellt von anonym am Sonntag 10. Februar 2019, 12:46
I guess both are optional, but both could be part of the exam.

---

erstellt von anonym am Sonntag 10. Februar 2019, 12:46
maybe everything is optional, but will be part of the exam

---

erstellt von anonym am Sonntag 10. Februar 2019, 13:25

Optionality is hard to define (see "family resemblances"), so you have to consider following table with 1-anonymity and 1-diversity:

topic	optional	rly optional?
intro	yes	no
chap 1	yes	no
chap 2	yes	no
chap 3	yes	no
diff. priv.	yes	no

Kein Titel

erstellt von Fabian Kügler am Sonntag 10. Februar 2019, 14:27

As far as I remember, the Intro slides are NOT mandatory. However, if you have problems with the other topics you can learn those slides as well an tell him that you learnt them and he will then ALSO (not only) ask you about that chapter. The differential privacy as well as the other sets of slides are of course not optional.

By the way if you had a look at the first slides of the Intro chapter it literally says that it is not relevant for the exam (except a few points which are marked which I could however not find)

Best
Fabian

Thema: Zero-Knowledge Proof

erstellt von anonym am Sonntag 10. Februar 2019, 19:51

Hi,
Can someone help me with the 'Ali baba' cave example that was discussed during the 'Zero-Knowledge Proof' topic? I remember that the proof is not transferable in this case, but I don't recall what was the proof exactly?

Thanks!

No title
erstellt von Denis Arnst am Sonntag 10. Februar 2019, 20:06

This picture
helps: https://de.wikipedia.org/wiki/Zero-Knowledge-Beweis#/media/File:Zero_knowledge_cave_1.svg
You stand at position 3. You want to know from some person (B) if he knows how to get through the gate at 1/2. The person B can prove to you that he knows how to get through the gate, by simply going into Position 2 (right side) and coming out of Position 1 (left side). As you can't see how B opens the gate, you don't know the secret, but you know that B must know it.
It is not transferable as a person in position 4 doesn't know wether B really did this experiment (even a movie of B doing it could be cut/faked).

---

erstellt von anonym am Sonntag 10. Februar 2019, 20:40

Great! Exactly what I needed. Thanks a lot!

---

erstellt von Denis Arnst am Sonntag 10. Februar 2019, 20:56

One more hint: My example is simplified. The original proof works by statistical means. You stand outside the cave, and B goes into 1 or 2. You go to 3 and make a challenge to B, that she should return on either 1 or 2 (you specify the return path). Note that the probability of someone solving one iteration of the experiment is 50%. You'll repeat this experiment several times. Now, if B does this n times right, the probability that B knows the secret is 1-(2)^(-n)
