Topics in Algebra: Cryptography - Blatt 6

11.30-12:15, Seminarraum 9, Oskar-Morgenstern-Platz 1, 2.Stock

http://www.mat.univie.ac.at/~gagt/crypto2018

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. a) What other uses of cryptographic proofs-of-work do you know?

b) What are (dis)advantages of deploying distributed ledgers?

Question 2. What is the length (=number of intermediate hash values) of a verification path in the Merkle tree having n transations? What is it for a k-ary tree with n leaves?

Question 3. Why in your opinion is the difficulty of the proof-of-work in bitcoin set to 10 minutes? What would go wrong if it was changed to 60 minutes or 10 seconds?

2 Exercises

Question 4. Let h be an arbitrary hash function with 256-bit output. Show that choosing $2^{130} + 1$ inputs uniformly at random gives a 99.966% chance to have at least two inputs that collide.

Hint: use the probabilistic version of the pidgeonhole principle (see also the birthday paradox).

Question 5. How secure is a Merkle tree? Can we forge messages, and if so what kind of forgeries can we construct?

3 Further notes on hash functions

I've been reading:

1. https://news.ycombinator.com/item?id=12494317

2. https://crypto.stackexchange.com/questions/9684/pre-image-resistant-but-not-2nd-pre-image-resistant

Take a look at the discussions there for more information. Note, they're hyperlinked in the electronic version of this document.