

Topics in Algebra: Cryptography - Blatt 4

<http://www.mat.univie.ac.at/~gagt/crypto2019>

Goul'nara Arzhantseva	Martin Finn-Sell
goul'nara.arzhantseva@univie.ac.at	martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. i) Why does ElGamal produce **two** components of ciphertext?

ii) Why are the exponents used for decryption smaller for ElGamal compared to RSA?

iii) Why is ECC more popular than the original ElGamal?

Question 2. Which of the following statements is true:

i) Breaking ElGamal is equivalent to solving “Asymmetry of ElGamal”;

ii) ElGamal is less efficient for encryption than RSA;

iii) ElGamal is more efficient for decryption than RSA;

iv) There is no message expansion in the RSA-OAEP cryptosystem.

Question 3. Prove the Cayley–Bacharach theorem.

Question 4. a) What other uses of cryptographic proofs-of-work do you know?

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

Question 5. What is the length (=number of intermediate hash values) of a verification path in the Merkle tree having n transactions? What is it for a k -ary tree with n leaves?

Question 6. 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 7. State and illustrate both the pigeonhole principle and the probabilistic pigeonhole principle. Explain the applications of both.

Question 8. 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.

Question 9. How secure is a Merkle tree? Can we forge messages, and if so what kind of forgeries can we construct?