Topics in Algebra: Cryptography - Test Questions

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. Give an example of an application where

i) entity authentication and data origin authentication are both required;

ii) data origin authentication is required but not data integrity.

Question 2. If a given key of a Vingère cipher has repeated letters, does it make it any easier to break?

Question 3. Invent and analyse an affine cipher (i.e consider length, size, attacks etc).

Question 4. How long (in years, days, hours, seconds) will it take 1000000 computers each processing 1000000 operations per second to

i) multiply two 1000-bit numbers together;

ii) perform an exhaustive search for a 128-bit key;

iii) find the correct key (on average) while performing a brute force attack on a 128-bit key.

Question 5. i) Does a one time pad retain perfect secrecy if we reuse the same key twice?

ii) Has a Vingère cipher got perfect secrecy?

iii) Could we use one time pads in practice?

Question 6. What is the complexity of the RSA parameter generation?

Question 7. Let f be a one-way function. Is $\mathsf{f} \circ \mathsf{f}$ necessarily a one-way function?

Question 8. What is the worst case / average case complexities of trial division?

Question 9. Design an algorithm for computing the square root of an integer. What about its complexity? What about its modular variant and its complexity?

Question 10. Which of the following statements are true?

1. If the RSA cryptosystem is breakable, then large numbers can be factored;
2. Breaking the ECC cryptosystem is equivalent to solving the discrete logarithm problem;
3. There is no message expansion in the ECC cryptosystem.

Question 11. Why in practice public-key cryptosystems have longer key lengths than symmetric cryptosystem?

Question 12. Give a proof of Theorem 2 from the Annex notes for Chapter 2.

Question 13. 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 14. 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 15. Prove the Cayley–Bacharach theorem.

Question 16. a) What other uses of cryptographic proofs-of-work do you know?

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

Question 17. 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 18. 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?

Question 19. a) What other uses of cryptographic proofs-of-work do you know?

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

Question 20. 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 21. 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?

Question 22. Is the k given in the example of the LFSR the period?

Question 23. Show that the matrix obtained from the linear equations of the Linear Feedback Shift register is invertible mod 2.

Question 24. Consider the LFSR as a bit generator. What are, in this case, the values of k and l for the definition of a bit generator?