Topics in Algebra: Cryptography - Blatt 1

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?

2 Exercises

Question 6. Determine whether or not the Caesar cipher has perfect secrecy.

Question 7. Describe 3 elements of the set $\mathcal{K}$ in the definition of RSA encryption for the primes $p = 7$ and $q = 11$, that is generate three public and private key pairs. Use those elements to simulate the sending of the message 42, and describe the steps in detail where appropriate.

Question 8. For $n = pq$, where p and q are distinct primes, consider:

$$\lambda(n) = \frac{\phi(n)}{\gcd(p-1, q-1)}.$$

Suppose we modify the RSA cryptosystem by asking that $ab = 1 \mathrm{mod} \lambda(n)$.

i) show that the encryption and decryption are well defined operations in this new system;

ii) for $p = 37$, $q = 79$, and $b = 7$ compute a in this modifed RSA system. How does it compare to the value in the original RSA scheme?

Question 9. Prove that RSA is vulnerable (i.e insecure to) a chosen cipher text attack. In particular, given a cipher text y, describe how to choose $\tilde{y} \neq y$ such that knowledge of the plaintext $\tilde{x} = D_{\mathcal{K}}(\tilde{y})$ allows $x = D_{\mathcal{K}}(y)$ to be computed.