# Magma Assignment 05

Combinatorics and Cryptography

## Textbook RSA

Write a Magma code for solving the following RSA-related problem(s). Factorizing the RSA-modulus using `Factorization` (or similar) is forbidden.

The public parameters of the tasks (blue values) are available in the attached file `assignment5_variables.magma`. You can also load[1] the variables in you work terminal using

```
> load"assignment5_variables.magma";
```

## Task 1 [3 pts.]

Assume cA is using the RSA public-key pair $n_1$ = `GenModulus`(512), $e_1$, and that you manage to obtain the private key $d_1$. Determine the factorization of $n_1$.

Solve the task by implementing a Magma function called `FactorsFromD` which, on inputs $(n, e, d)$, always returns $(p, q)$, i.e. the factorization of the RSA-modulus $n$. The function will be tested also on other inputs.

## Task 2 [not mandatory]

Assume that cA is using the RSA public-key pair $n_2$ = `GenModulus`(512), $e_2 = 3$. You have intercepted a ciphertext $c = m^3 \bmod n2$. Try to recover the plaintext $m$.

## Points

Submitting a working solution for Task 1 will give you up to three points.

[1] writing the complete file address may be required