ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, SPRING 2023, assignments list # 7, 27.4.2023

1. What are the consequences of reusing the initial vector IV in case of the GCM mode?
2. Consider a modification of the GCM mode, in which GHASH is not truncated in the last step but the MAC consists of all 128 bits. Is it more secure or not?
3. Create an attack against a version of GCM where the last iteration of GHASH is skipped (the one where we use the lengths of A and C).
4. Consider the Ferguson attack against GCM. Describe the details of calculating $c \cdot x$ for a constant $c \in \mathrm{GF}(2^{128})$ and $x \in \mathrm{GF}(2^{128})$ by matrix multiplication. How do we create the matrix corresponding to a constant c?

   Describe in detail how to calculate the matrix used for the operation $x \to x^2$.

/-/ Mirosław Kutyłowski