**Report – first phase of the project**

Martin Bulák, Michal Čech, Šimon Doucha

Scripts and generator: https://github.com/michal-cech/PV204-Project/

Keys: https://drive.google.com/drive/folders/1efLlZsRKriTyoDMFVR38LwZjzIF5dokN?usp=sharing

We are working with BearSSL library<https://bearssl.org/> which is a cryptographic library implemented by Thomas Pornin. The author says that the library is considered beta-quality and some features are missing.