The goal of this thesis is to present the problem of implementation of user-friendly and practical cryptosystem based on algorithms that are intractable by quantum computing. Resulting software is expected to use code-based cryptography (McEliece-based cryptosystems) to the highest possible extent while maintaining similarity with already-existing cryptographical applications (GnuPG).