Table of Contents

[1 Introduction 1](#_Toc147160248)

[2 Block ciphers 2](#_Toc147160249)

[2.1 Common general principles 2](#_Toc147160250)

[2.2 ECB – Electronic Code Book 3](#_Toc147160251)

[2.3 CBC – Cipher Block Chaining 3](#_Toc147160252)

[2.4 GCM – Galois-Counter Mode 3](#_Toc147160253)

[3 Comparison of modes 4](#_Toc147160254)

[4 Selected flaws and vulnerabilities 5](#_Toc147160255)

[5 Conclusions 6](#_Toc147160256)

[References 7](#_Toc147160257)