

PLAYING IN A SANDBOX WITH AUTHENTICATED SECURITY

(700100)

*700100: SHORT NOTE*

*TRUSTWORTHY COMPUTING*

*18 MAY 2020*

Farah Aly - 201505395

Contents

[Introduction 1](#_Toc40050835)

[Concept of Authenticated Encryption Modes 1](#_Toc40050836)

[Concept of Generic Composition Methods of Authenticated Encryption Modes 1](#_Toc40050837)

[Single-Pass Authenticated Encryption Modes 1](#_Toc40050838)

[Conclusion 1](#_Toc40050839)

[References 2](#_Toc40050840)

[Appendix 2](#_Toc40050841)

# Introduction

# Concept of Authenticated Encryption Modes

<https://blog.cryptographyengineering.com/2012/05/19/how-to-choose-authenticated-encryption/>

# Concept of Generic Composition Methods of Authenticated Encryption Modes

<https://crypto.stackexchange.com/questions/8812/how-to-build-a-secure-ae-scheme-with-generic-composition>

# Single-Pass Authenticated Encryption Modes

<https://crypto.stackexchange.com/questions/33684/difference-between-mac-and-authenticated-encryption>

# Conclusion

# References

# Appendix