UNIVERSITY OF PISA

MASTER'S DEGREE IN COMPUTER ENGINEERING

Foundations of Cybersecurity

Bulletin-Board-System

Professor:

Gianluca Dini

Student:

Giovanni Ligato

Index

1. Introduction
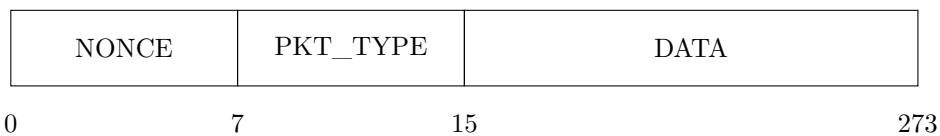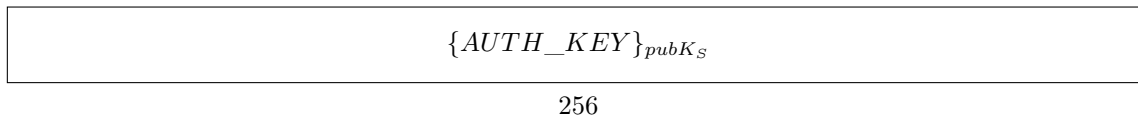
AAAAAA

NONCE	PKT_TYPE	DATA

0　　　　　　　　7　　　　　　　15　　　　　　　　　　　　　　　273

First packet:

$\{AUTH\_KEY\}_{pubK_S}$

256

Second packet:

IV	AAD	TAG

12　　　　　　　　　　　　670　　　　　　　　　　　　　16

IV	AAD_SIZE	AAD	CIPH_SIZE	CIPH	TAG

12　　　　4　　　AAD_SIZE　　　4　　　CIPH_SIZE　　　16