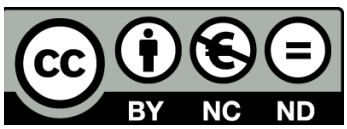
Crypto Go – Symmetric key – English (open source)

Authors:	Ana Isabel González-Tablas Ferreres. COSEC Lab, Universidad Carlos III de Madrid. María Isabel González Vasco. Departamento MACIMTE, Universidad Rey Juan Carlos.
Copyright:	Crypto Go game is property of Universidad Carlos III de Madrid and Universidad Rey Juan Carlos. It is registered as “obra científica.” ©Copyright 2018. All rights reserved.

Herein we publish a print-and-play version of Crypto Go cards, under license CC BY-NC-ND.



This document contains print-and-play cards of one of the cryptographic card types or of auxiliary cards. Printing configuration: 9 pages per page, one-side, A4 size, Black/White or as desired.

File name	Content and instructions
Open_AE_EN	AE cards. Print on green paper.
Open_BC_EN	BC cards. Print on pink paper.
Open_H_EN	H cards. Print on orange paper.
Open_MAC_EN	MAC cards. Print on blue paper.
Open_OM_EN	OM cards. Print on yellow paper.
Open_SC_EN	SC cards. Print on red paper.
Open_Auxiliares_EN	Auxiliary cards. Print on white paper.

How to cite the game:

González-Tablas Ferreres, A. I. y González Vasco, M. I. (2018). *Crypto Go* : Symmetric key – English (open source) [Card game]. Madrid : Universidad Carlos III de Madrid, Universidad Rey Juan Carlos. Available at http://hdl.handle.net/10016/28433

AE 1

CCM

Standarized by NIST in 2004. It combines CTR mode with CBC-MAC.

Authenticated encryption

AE 1

CWC

Designed by Kohno et al.
in 2004, it combines a
Carter-Wegman MAC with
CTR mode encryption.

Authenticated encryption

AE 1

GCM

Galois Counter Mode was designed by McGrew and Viega in 2004. It combines CTR mode with a Carter-Wegman MAC.

Authenticated encryption

Generic Composition

Generic combination of an encryption scheme with a MAC. It follows the encrypt-then-MAC paradigm.

AE 1

OCB

The Offset Codebook mode was proposed by Rogaway et al. in 2003. From 2013 it is partially free (e.g. for sofware usage under a GNU General Public Licence)

Authenticated encryption

AE 1

EAX

Introduced by Bellare et al. in 2004, it is very similar to CCM mode. Both encryption and decryption can be performed online.

Authenticated encryption

AE 1

EAX

Introduced by Bellare et al. in 2004, it is very similar to CCM mode. Both encryption and decryption can be performed online.

Authenticated encryption