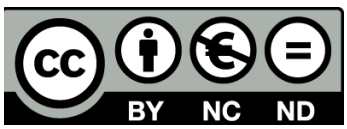
Crypto Go – Symmetric key – English (open source)

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

OM 2c 2d

CFB

Cipher Feedback mode.
Standarized in 2001.

Operation mode

OM 2c 2d

OFB

Output Feedback mode.
Standarized in 2001.

Operation mode

OM 2c 2d

CBC

Cipher Block Chaining mode. Widely deployed since its standarization in 2001.

Operation mode

OM 2c 2d

CBC

Cipher Block Chaining mode. Widely deployed since its standarization in 2001.

Operation mode

OM 2c 2d

CTR

Counter mode.
Standarized in 2001.

Operation mode

OM 2c 2d

CTR

Counter mode.
Standarized in 2001.

Operation mode

OM 2c 2d

ECB

Electronic Code Book is the simplest operation mode, treating each ciphertext block independently.

Operation mode

OM 2c 2d

ECB

Electronic Code Book is the simplest operation mode, treating each ciphertext block independently.

Operation mode

OM 2c 2d

EME

ECB-mask-ECB is a mode designed by Halevi and Rogaway in 2004.

Operation mode

OM 2c 2d

EME

ECB-mask-ECB is a mode designed by Halevi and Rogaway in 2004.

Operation mode

OM 2c 2d

FFX

Format preserving symmetric encryption mode. Proposed by Bellare et al., and standarized in 2016.

Operation mode

OM 2c 2d

FFX

Format preserving symmetric encryption mode. Proposed by Bellare et al., and standarized in 2016.

Operation mode

OM 2c 2d

FFX

Format preserving symmetric encryption mode. Proposed by Bellare et al., and standarized in 2016.

Operation mode