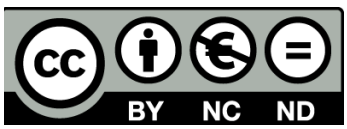
Crypto Go – Symmetric key – English (open source)

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

MAC 2a 2b 2c 2d

AMAC

Known as ANSI Retail MAC, it is used in combination with DES.

Authentication code

MAC 2a 2b 2c 2d

AMAC

Known as ANSI Retail MAC, it is used in combination with DES.

Authentication code

MAC 2a 2b 2c 2d

AMAC

Known as ANSI Retail MAC, it is used in combination with DES.

Authentication code

MAC 2a 2b 2c 2d

AMAC

Known as ANSI Retail MAC, it is used in combination with DES.

Authentication code

MCA 2a 2b 2c 2d

CMAC

Proposed by Iwata and Kurosawa, and standarized in 2011. It is used in combination with a block cipher.

Authentication code

MCA 2a 2b 2c 2d

CMAC

Proposed by Iwata and Kurosawa, and standarized in 2011. It is used in combination with a block cipher.

Authentication code

MCA 2a 2b 2c 2d

CMAC

Proposed by Iwata and Kurosawa, and standarized in 2011. It is used in combination with a block cipher.

Authentication code

MCA 2a 2b 2c 2d

CMAC

Proposed by Iwata and Kurosawa, and standarized in 2011. It is used in combination with a block cipher.

Authentication code

MCE 2a 2b 2c 2d

EMAC

Proposed by Petrank and Rackoff, and standarized in 2011. It is used in combination with a BC.

Authentication code

MCE 2a 2b 2c 2d

EMAC

Proposed by Petrank and Rackoff, and standarized in 2011. It is used in combination with a BC.

Authentication code

MCE 2a 2b 2c 2d

EMAC

Proposed by Petrank and Rackoff, and standarized in 2011. It is used in combination with a BC.

Authentication code

MCE 2a 2b 2c 2d

EMAC

Proposed by Petrank and Rackoff, and standarized in 2011. It is used in combination with a BC.

Authentication code

MAC 2a 2b 2c 2d

GMAC

MAC underlying the authenticated encryption mode GCM.

Authentication code

MAC 2a 2b 2c 2d

GMAC

MAC underlying the authenticated encryption mode GCM.

Authentication code

MAC 2a 2b 2c 2d

GMAC

MAC underlying the authenticated encryption mode GCM.

Authentication code

MAC 2a 2b 2c 2d

GMAC

MAC underlying the authenticated encryption mode GCM.

Authentication code

MAC 2a 2b 2c 2d

HMAC

Proposed by Bellare et al. in 1997, and standarized several times. It is used in combination with a secure hash.

Authentication code

MAC 2a 2b 2c 2d

HMAC

Proposed by Bellare et al. in 1997, and standarized several times. It is used in combination with a secure hash.

Authentication code

MAC 2a 2b 2c 2d

HMAC

Proposed by Bellare et al. in 1997, and standarized several times. It is used in combination with a secure hash.

Authentication code

MAC 2a 2b 2c 2d

HMAC

Proposed by Bellare et al. in 1997, and standarized several times. It is used in combination with a secure hash.

Authentication code

MAC 2a 2b 2c 2d

Poly1305

Polynomial-based Carter-Wegman MAC.

Authentication code

MAC 2a 2b 2c 2d

Poly1305

Polynomial-based Carter-Wegman MAC.

Authentication code

MAC 2a 2b 2c 2d

Poly1305

Polynomial-based Carter-Wegman MAC.

Authentication code

MAC 2a 2b 2c 2d

Poly1305

Polynomial-based Carter-Wegman MAC.

Authentication code

MAC 2a 2b 2c 2d

UMAC

Proposed by Black et al. in 1999. It is implemented with an Universal Hash Function (UHF).

Authentication code

MAC 2a 2b 2c 2d

UMAC

Proposed by Black et al. in 1999. It is implemented with an Universal Hash Function (UHF).

Authentication code

MAC 2a 2b 2c 2d

UMAC

Proposed by Black et al. in 1999. It is implemented with an Universal Hash Function (UHF).

Authentication code

MAC 2a 2b 2c 2d

UMAC

Proposed by Black et al. in 1999. It is implemented with an Universal Hash Function (UHF).

Authentication code