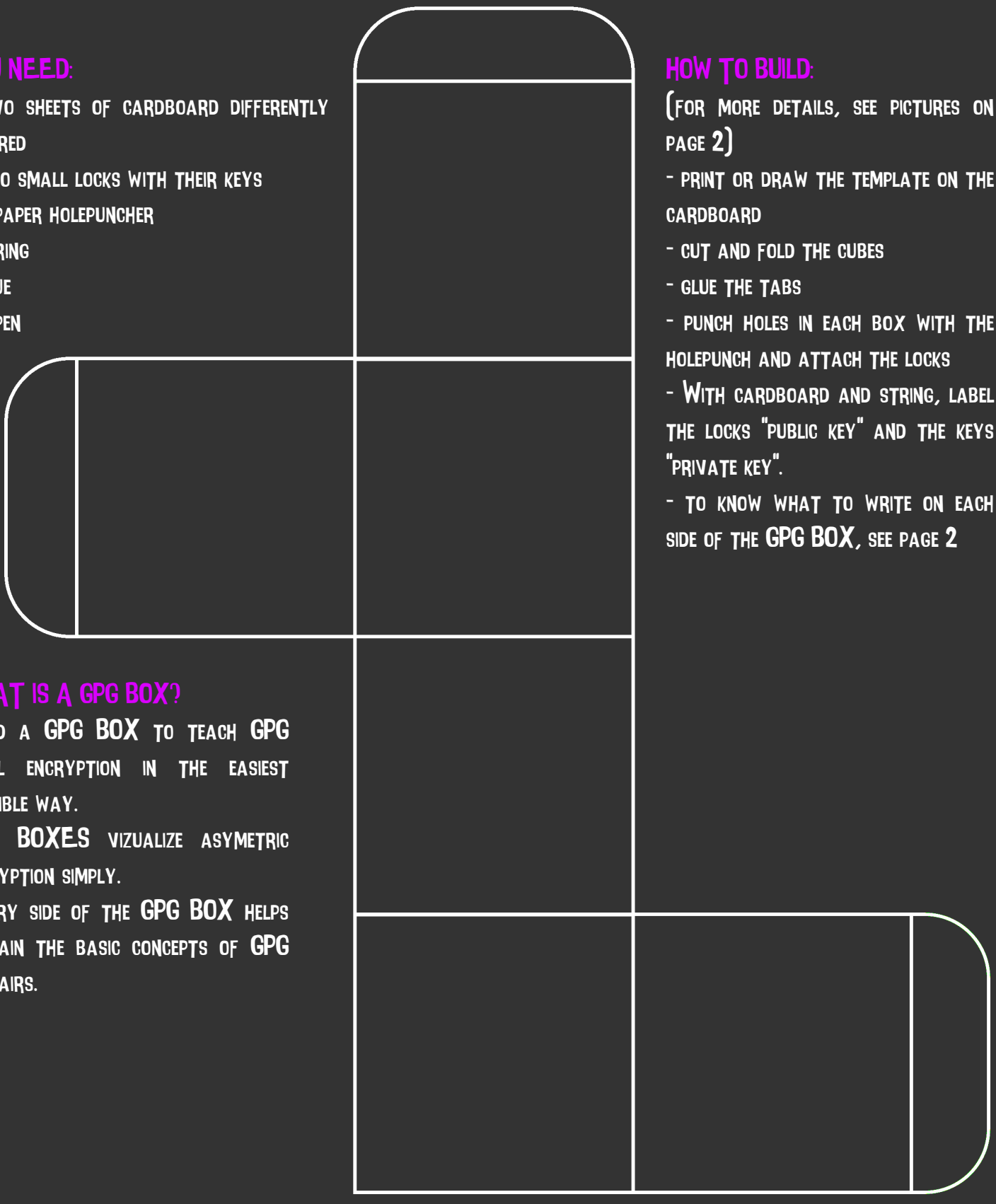
BUILD YOUR OWN GPG BOX!

HOW TO TEACH EMAIL ENCRYPTION

YOU NEED:

- TWO SHEETS OF CARDBOARD DIFFERENTLY COLORED
- TWO SMALL LOCKS WITH THEIR KEYS
- A PAPER HOLEPUNCHER
- STRING
- GLUE
- A PEN



HOW TO BUILD:

(FOR MORE DETAILS, SEE PICTURES ON PAGE 2)

- PRINT OR DRAW THE TEMPLATE ON THE CARDBOARD
- CUT AND FOLD THE CUBES
- GLUE THE TABS
- PUNCH HOLES IN EACH BOX WITH THE HOLEPUNCH AND ATTACH THE LOCKS
- WITH CARDBOARD AND STRING, LABEL THE LOCKS "PUBLIC KEY" AND THE KEYS "PRIVATE KEY".
- TO KNOW WHAT TO WRITE ON EACH SIDE OF THE GPG BOX, SEE PAGE 2

WHAT IS A GPG BOX?

BUILD A GPG BOX TO TEACH GPG EMAIL ENCRYPTION IN THE EASIEST POSSIBLE WAY.

GPG BOXES VIZUALIZE ASYMETRIC ENCRYPTION SIMPLY.

EVERY SIDE OF THE GPG BOX HELPS EXPLAIN THE BASIC CONCEPTS OF GPG KEYPAIRS.

"GPG BOX" TUTORIAL BY @NSMNSR & @SHIROMARIEKE FOR CRYPTOPARTY

SIDE 1: METADATA

- GPG encrpytion doesn't come with anonymity.
- Only the **CONTENT** of your message is encrypted. Important information remains unencrypted and can be read by third parties: time and location, identity of the sender and reciever, etc.
- **BE CAREFUL**: The email subject line is never encrypted. Do not send any important information in this line.

SIDE 2: CREATION DATE AND EXPIRATION DATE

- Generate keypairs with an **EXPIRATION DATE**. Your private key can be compromised. An expiration date of a few years limits the value of stealing your keys.

SIDE 3: FINGERPRINT AND KEY ID

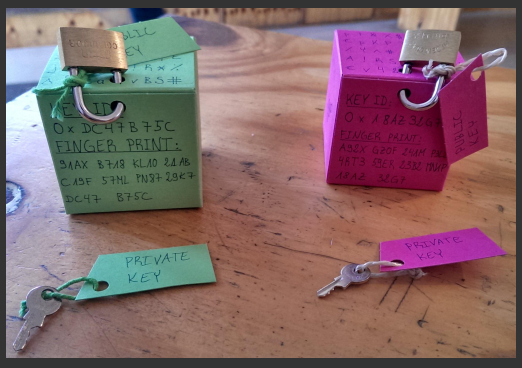
- Each keypair has a **UNIQUE** fingerpint and key id.
- The **KEY ID** consists of the last characters of the fingerprint. It is the name of the key. It can be used to find someone's public key on a keyserver.
- The **FINGERPRINT** is a string of **40** characters. It is used to **VERIFY** a public key belongs to a particular person. To ultimately check a fingerprint, meet its owner in person.

SIDE 4: SIGNATURE

- Sign your emails with your private key. A **SIGNATURE** proves that you are the author of the message and that it has not been modified.

SIDE 5: ENCRYPTED MESSAGE

- An **ENCRYPTED** message looks like a random string of numbers, letters and special characters.



LOCKS & KEYS

- When you send an email, you **ENCRYPT** it with the other person's public key. You **SIGN** it with your private key.
- When you recieve an email, you **DECRYPT** it with your private key. You **VERIFY** it's signature with the other person's public key.

"GPG BOX" tutorial by @NSMNSR & @SHIROMARIEKE for CRYPTOPARTY