

# Block Ciphers

Rohit Musti

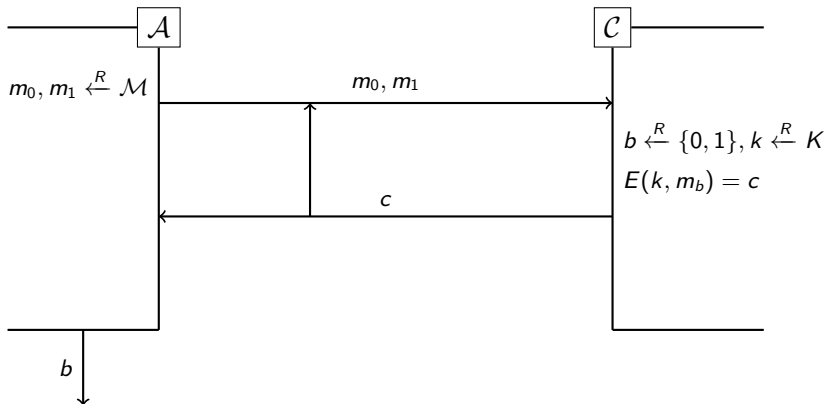
CUNY - Hunter College

February 18, 2022

# Overview

- We just introduced the concept of stream ciphers and used PRGs to create a basic construction
- We also introduced security games
- In this lecture, we will build on these ideas and introduce the block cipher a practical cryptography system

# One Time Pad Security Game: Chosen Plaintext Attack



# Pseudo Random Functions (PRFs)

- $F : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$
- this function must be efficient
- this function is not necessarily one-to-one
- this function is not necessarily invertable

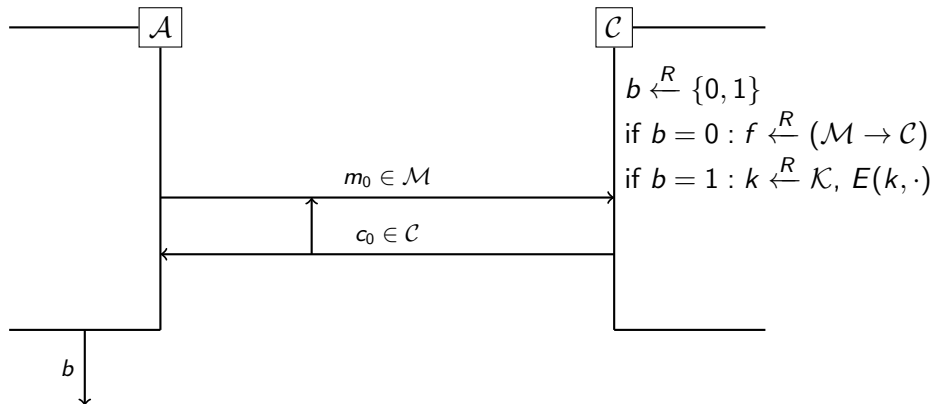
# Pseudo Random Permutation (PRPs)

- $P : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$
- this function must be efficient
- this function is one-to-one
- there exists an efficient algorithm for inverting this

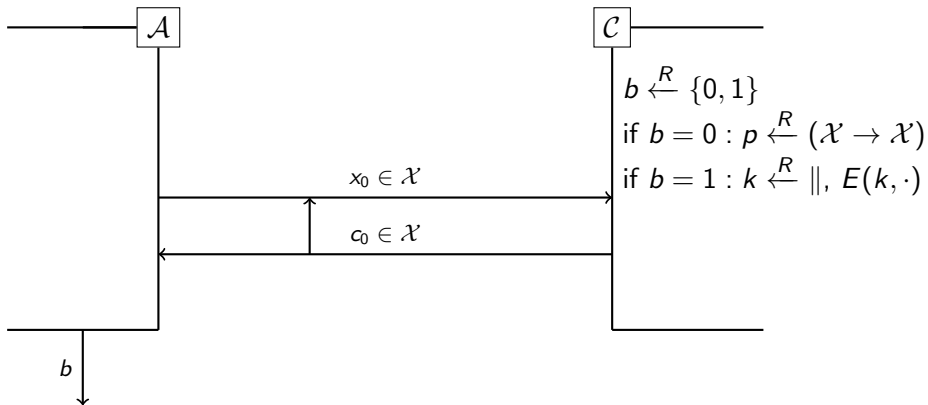
# Security of PRPs and PRFs

- A PRF  $F : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$  is secure if  $F(k, \cdot)$  is indistinguishable from a random function  $f \xleftarrow{R} (\mathcal{M} \rightarrow \mathcal{C})$
- a PRP  $P : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$  is secure if  $P(k, \cdot)$  is indistinguishable from a random permutation  $p \xleftarrow{R} (\mathcal{X} \rightarrow \mathcal{X})$

# PRF Security Game: Chosen Plaintext Attack



# PRP Security Game: Chosen Plaintext Attack





# Security Lemma

- a secure PRP is equivalent to a secure PRF

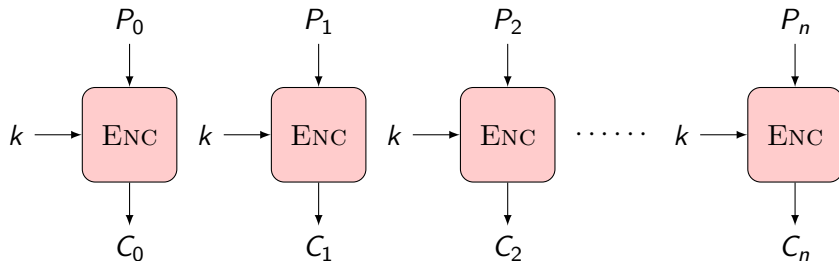
# Block Ciphers

- block ciphers can be thought of as PRPs
- block ciphers are deterministic ciphers  $\mathcal{E} = (E, D)$
- its message space and ciphertext space are the same:  $\mathcal{M} = \mathcal{C}$
- Shares the correctness requirement with Shannon Ciphers  
 $D(k, E(k, m)) = m$

# History: Electronic Code Book

- Developed by IBM in the 1970s, became an official Federal Information Processing Standard in 1977
- Released with 4 other ciphers, all of which were more secure, but not totally secure on their own
- Name derives the code books used during the Civil War

## How it Works: Electronic Code Book



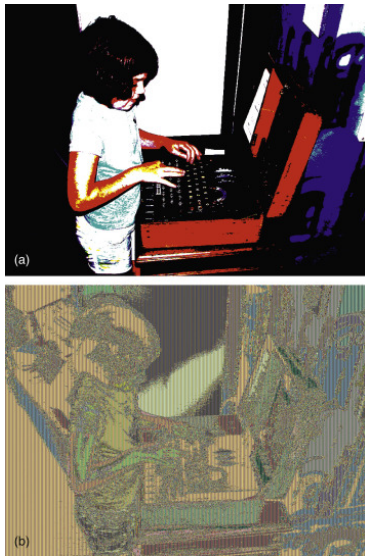
*Image Credit:* Diana Maimut

## Security Weakness: Electronic Code Book

- since the encryption function is a PRP, it is deterministic and one-to-one
- therefore, if  $m_1 = m_2$ , then it follows that  $c_1 = c_2$
- this doesn't achieve chosen plaintext attack security

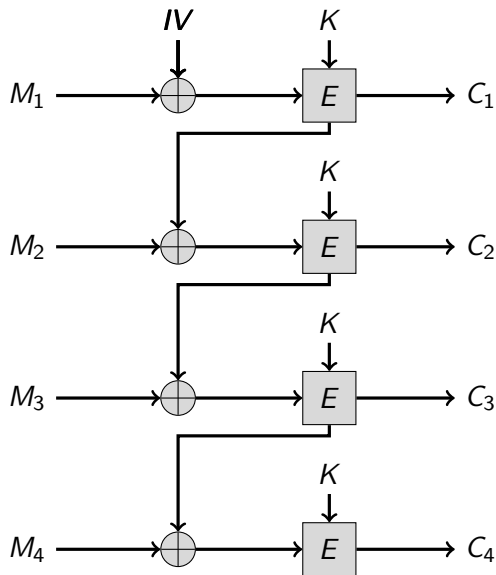
Future HW: describe an attack to break CPA given ECB

# Image Encryption using ECB



*Image Credit: (the NSA)*

# Cipher Block Chaining: CBC (not quite cryptocurrencies)

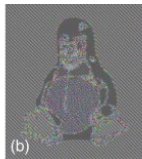


## CBC: Picking a good IV

- If you are developing a single use system, you do not even need an IV
- You can use a unique IV (i.e. counter mode) but then you have to sample a new IV each round, but you don't need to send the IV with the cipher text
- It is best to use a random IV every message and send it with the cipher text



# Image Encryption using CBC vs ECB



*Image Credit: (the NSA)*

# Data Encryption Standard (DES)

- IBM developed it with 128 bit keys and 128 blocks in 1970s
- the US National Beureau of Labor Standards requested a version of it (56 bit keys operating 64 bit blocks)
- widely criticized and speculated to have been made deliberately weak by certain US intelligence agencies
- Many fancy ways to break it, but you could brute force its 56 bit variant by 1998, now it can be brute forced in just 12 days

# Advanced Encryption System (AES)

- Developed by two belgian cryptographers, Joan Daemen and Vincent Rijmen
- Adopted by US government, supersedes DES (the one that contained EBC), in 2002
- First and only publicly accessible cypher approved by NSA

# AES: Algorithm

- ➊ Derive round keys using key scheduler from cipher key
- ➋ Expand the current key into the *round* key
- ➌ Complete encryption rounds
  - ➊ Non linear byte substitution according to look up table
  - ➋ Shift rows: last 3 rows are cyclically shifted
  - ➌ Mix Columns: combine four bytes in each column according to a linear mixing operation
  - ➍ XOR with round key
- ➍ Final encryption round
  - ➊ Non linear byte substitution according to look up table
  - ➋ Shift rows: last 3 rows are cyclically shifted
  - ➌ XOR with round key