Block Ciphers

Rohit Musti

CUNY - Hunter College

February 16, 2022

Overview

Overview

- We just introduced the concept of stream ciphers and used PRGs to create a basic construction

Overview

- We just introduced the concept of stream ciphers and used PRGs to create a basic construction
- We also introduced security games

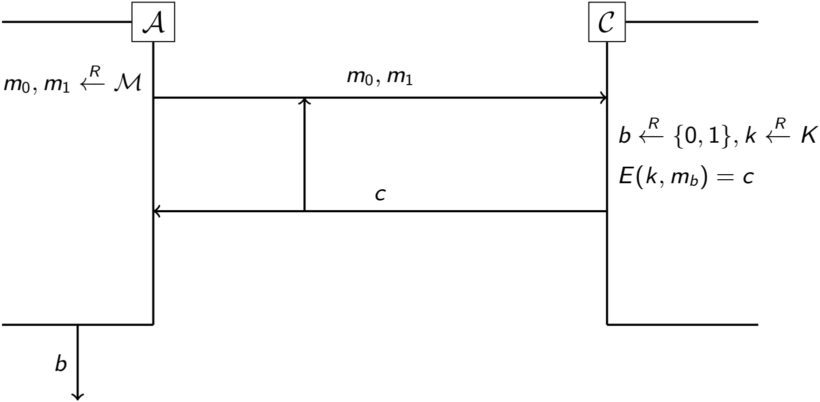
Overview

- 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

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


$\mathcal{A}$
$\mathcal{C}$
$m_0, m_1 \xleftarrow{R} \mathcal{M}$
m_0, m_1
$b \xleftarrow{R} \{0,1\}, k \xleftarrow{R} K$
$E(k, m_b) = c$
c
b

Pseudo Random Functions (PRFs)

Pseudo Random Functions (PRFs)

- $F : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

Pseudo Random Functions (PRFs)

- $F : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
- this function must be efficient

Pseudo Random Functions (PRFs)

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

Pseudo Random Functions (PRFs)

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

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)

Pseudo Random Permutation (PRPs)

- $P : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$

Pseudo Random Permutation (PRPs)

- $P : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$
- this function must be efficient

Pseudo Random Permutation (PRPs)

- $P : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$
- this function must be efficient
- this function is one-to-one

Pseudo Random Permutation (PRPs)

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

Pseudo Random Permutation (PRPs)

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

Security of PRPs and PRFs

Security of PRPs and PRFs

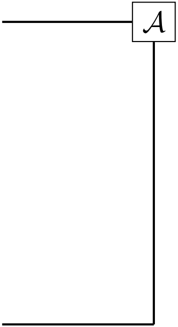
- A PRF $F : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ is secure if $F(k, \cdot)$ is indistinguishable from a random function $f \xleftarrow{R} (\mathcal{M} \to \mathcal{C})$

Security of PRPs and PRFs

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

PRF Security Game: Chosen Plaintext Attack

PRF Security Game: Chosen Plaintext Attack



PRF Security Game: Chosen Plaintext Attack

$\mathcal{A}$
$\mathcal{C}$

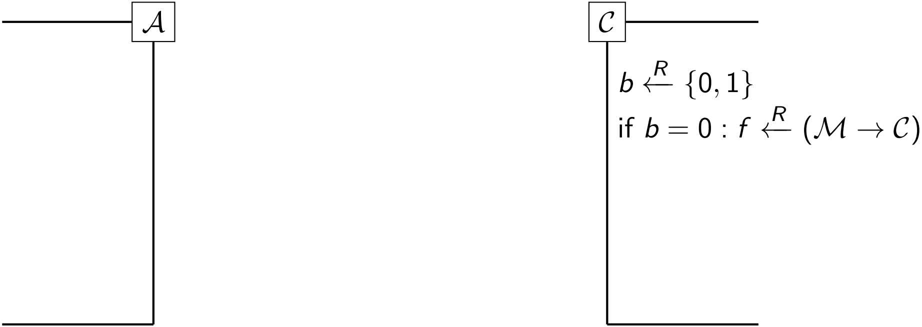
PRF Security Game: Chosen Plaintext Attack

$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

PRF Security Game: Chosen Plaintext Attack



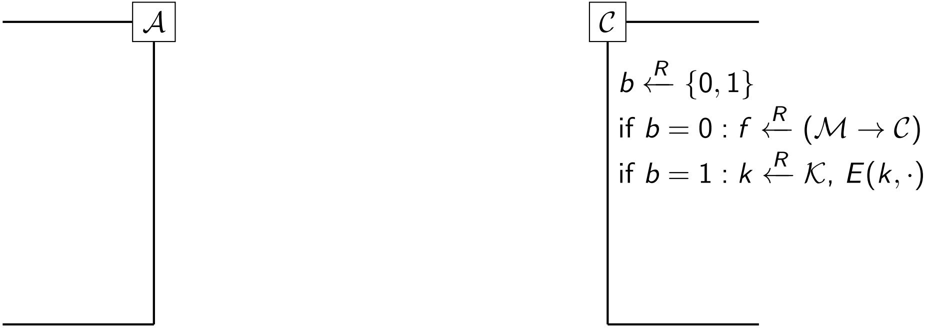
$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

if $b = 0 : f \xleftarrow{R} (\mathcal{M} \to \mathcal{C})$

PRF Security Game: Chosen Plaintext Attack

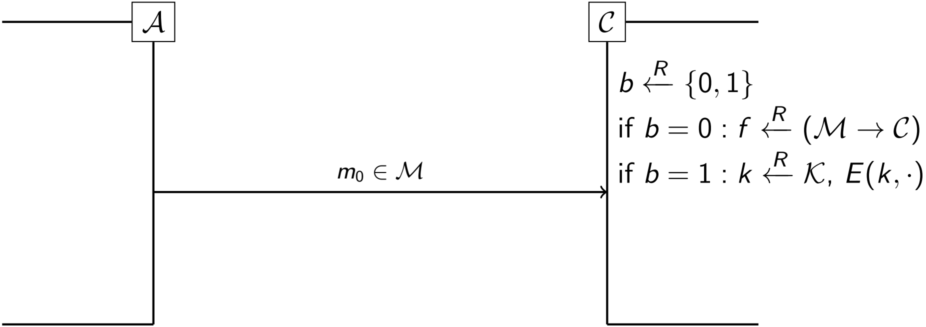


$b \xleftarrow{R} \{0,1\}$

if $b = 0 : f \xleftarrow{R} (\mathcal{M} \rightarrow \mathcal{C})$

if $b = 1 : k \xleftarrow{R} \mathcal{K},\ E(k, \cdot)$

PRF Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

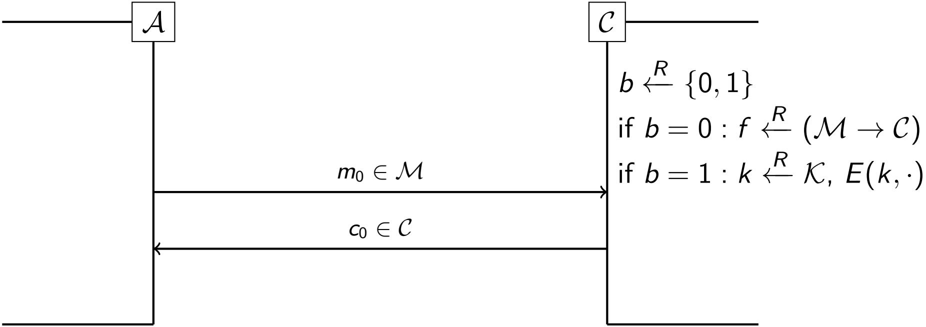
$b \xleftarrow{R} \{0,1\}$

if $b = 0 : f \xleftarrow{R} (\mathcal{M} \to \mathcal{C})$

if $b = 1 : k \xleftarrow{R} \mathcal{K},\ E(k, \cdot)$

$m_0 \in \mathcal{M}$

PRF Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

$b \overset{R}{\leftarrow} \{0,1\}$

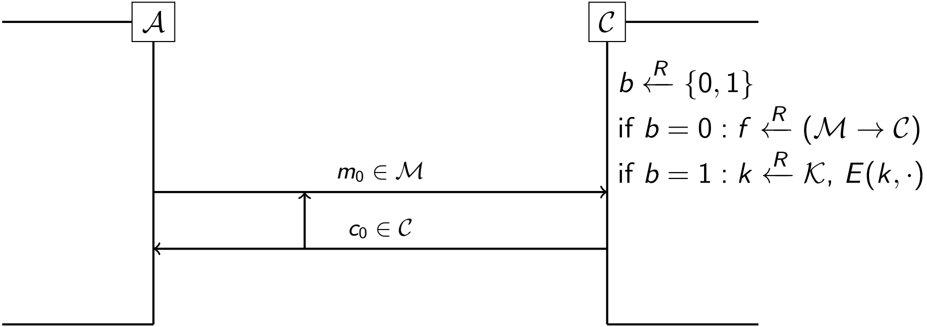
if $b = 0 : f \overset{R}{\leftarrow} (\mathcal{M} \rightarrow \mathcal{C})$

if $b = 1 : k \overset{R}{\leftarrow} \mathcal{K},\ E(k, \cdot)$

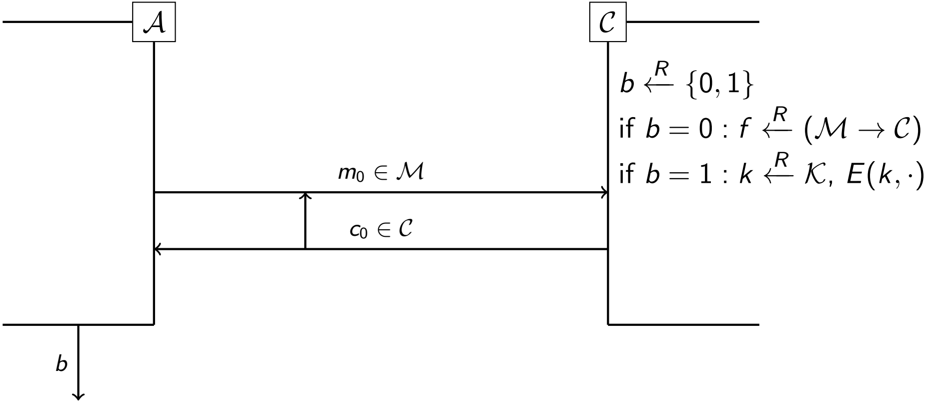
$m_0 \in \mathcal{M}$

$c_0 \in \mathcal{C}$

PRF Security Game: Chosen Plaintext Attack


$\mathcal{A}$
$\mathcal{C}$
$b \xleftarrow{R} \{0,1\}$
if $b = 0 : f \xleftarrow{R} (\mathcal{M} \to \mathcal{C})$
if $b = 1 : k \xleftarrow{R} \mathcal{K},\ E(k, \cdot)$
$m_0 \in \mathcal{M}$
$c_0 \in \mathcal{C}$

PRF Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

if $b = 0 : f \xleftarrow{R} (\mathcal{M} \to \mathcal{C})$

if $b = 1 : k \xleftarrow{R} \mathcal{K},\ E(k,\cdot)$

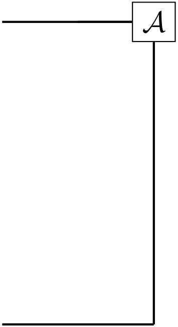
$m_0 \in \mathcal{M}$

$c_0 \in \mathcal{C}$

b

PRP Security Game: Chosen Plaintext Attack

PRP Security Game: Chosen Plaintext Attack

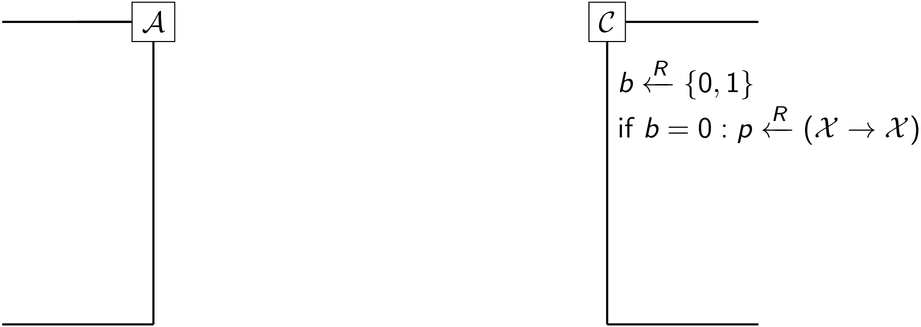


PRP Security Game: Chosen Plaintext Attack

PRP Security Game: Chosen Plaintext Attack

$\mathcal{A}$
$\mathcal{C}$
$b \xleftarrow{R} \{0,1\}$

PRP Security Game: Chosen Plaintext Attack



$b \xleftarrow{R} \{0, 1\}$

if $b = 0 : p \xleftarrow{R} (\mathcal{X} \to \mathcal{X})$

PRP Security Game: Chosen Plaintext Attack

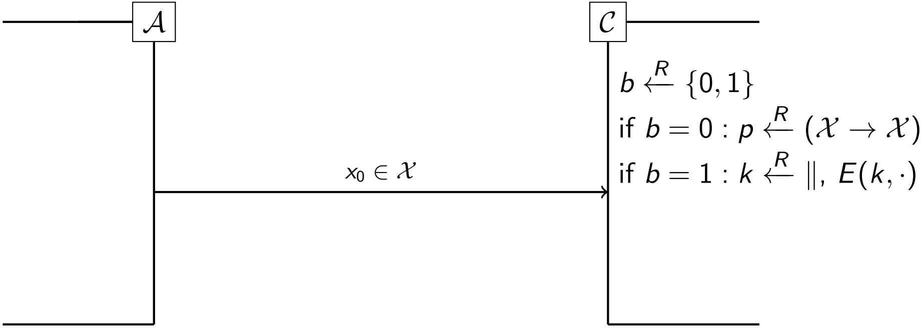
$\mathcal{A}$
$\mathcal{C}$

$b \xleftarrow{R} \{0, 1\}$

if $b = 0 : p \xleftarrow{R} (\mathcal{X} \to \mathcal{X})$

if $b = 1 : k \xleftarrow{R} \|$, $E(k, \cdot)$

PRP Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

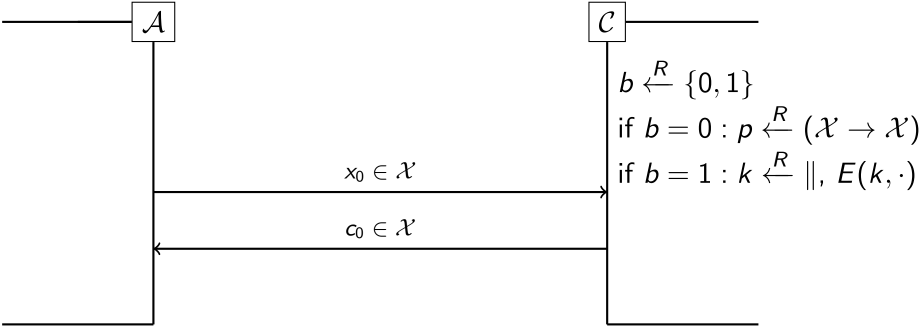
$b \xleftarrow{R} \{0,1\}$

if $b = 0 : p \xleftarrow{R} (\mathcal{X} \to \mathcal{X})$

if $b = 1 : k \xleftarrow{R} \|,\ E(k, \cdot)$

$x_0 \in \mathcal{X}$

PRP Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

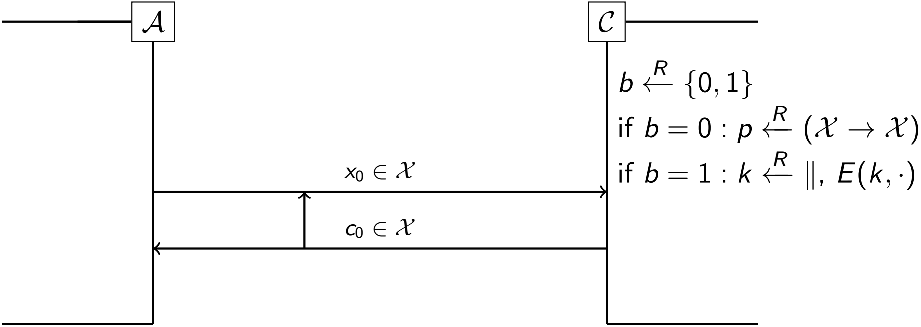
if $b = 0 : p \xleftarrow{R} (\mathcal{X} \rightarrow \mathcal{X})$

if $b = 1 : k \xleftarrow{R} \|, E(k, \cdot)$

$x_0 \in \mathcal{X}$

$c_0 \in \mathcal{X}$

PRP Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

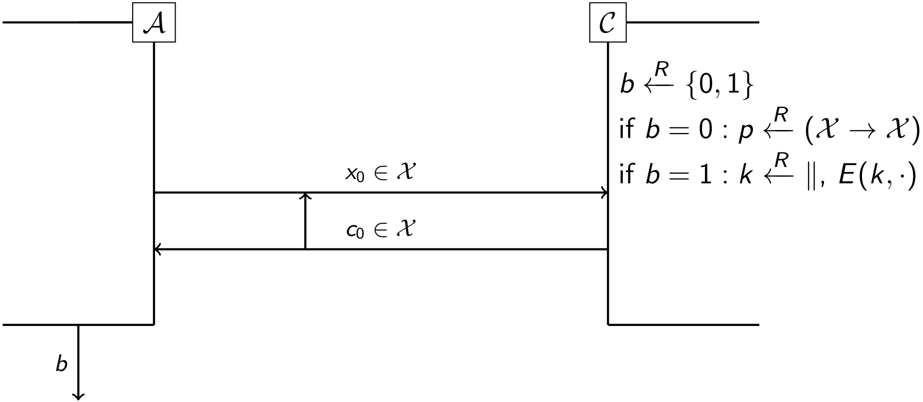
if $b = 0 : p \xleftarrow{R} (\mathcal{X} \to \mathcal{X})$

if $b = 1 : k \xleftarrow{R} \|, E(k,\cdot)$

$x_0 \in \mathcal{X}$

$c_0 \in \mathcal{X}$

PRP Security Game: Chosen Plaintext Attack



$\mathcal{A}$

$\mathcal{C}$

$b \xleftarrow{R} \{0,1\}$

if $b = 0 : p \xleftarrow{R} (\mathcal{X} \to \mathcal{X})$

if $b = 1 : k \xleftarrow{R} \|, E(k,\cdot)$

$x_0 \in \mathcal{X}$

$c_0 \in \mathcal{X}$

b

Security Lemma

- a secure PRP is equivalent to a secure PRF

Block Ciphers

Block Ciphers

- block ciphers can be thought of as PRPs

Block Ciphers

- block ciphers can be thought of as PRPs
- block ciphers are deterministic ciphers $\mathcal{E} = (E, D)$

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: $\mathcal{M} = \mathcal{C}$

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

History: Electronic Code Book

- Developed by IBM in the 1970s, became an official Federal Information Processing Standard in 1977

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

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

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

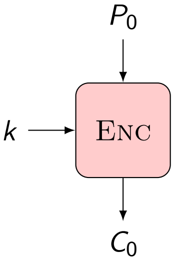


Image Credit: Diana Maimut

How it Works: Electronic Code Book

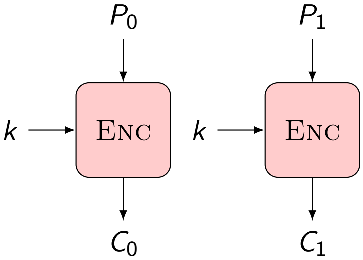


Image Credit: Diana Maimut

How it Works: Electronic Code Book

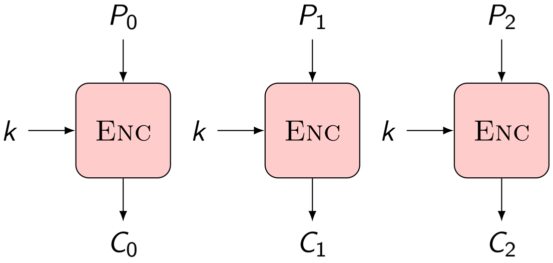


Image Credit: Diana Maimut

How it Works: Electronic Code Book

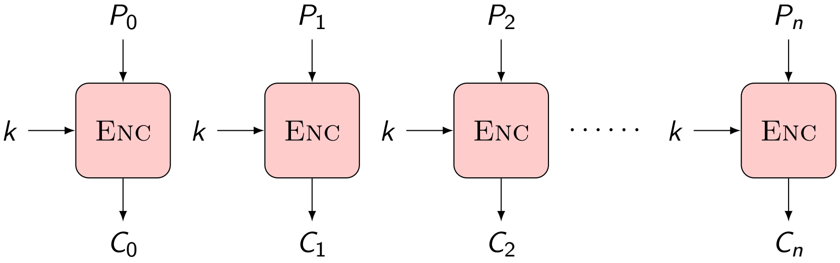


Image Credit: Diana Maimut

Security Weakness: Electronic Code Book

Security Weakness: Electronic Code Book

- since the encryption function is a PRP, it is deterministic and one-to-one

Security Weakness: Electronic Code Book

- since the encryption function is a PRP, it is deterministic and one-to-one
- therefore, it $m_1 = m_2$, then it follows that $c_1 = c_2$

Security Weakness: Electronic Code Book

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

Security Weakness: Electronic Code Book

- since the encryption function is a PRP, it is deterministic and one-to-one
- therefore, it $m_1 = m_2$, 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

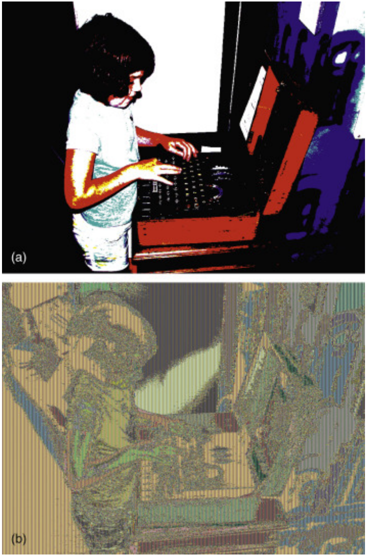


Image Credit: (the NSA)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

Image Credit: (Martin Thoma)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

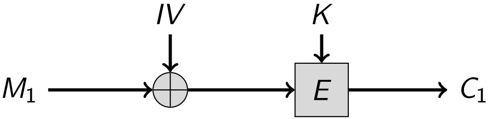


Image Credit: (Martin Thoma)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

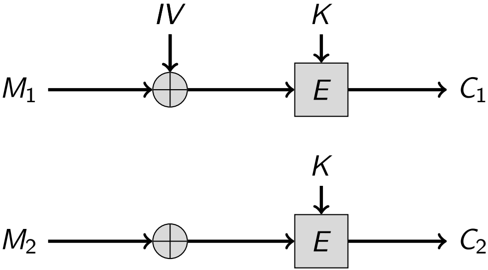


Image Credit: (Martin Thoma)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

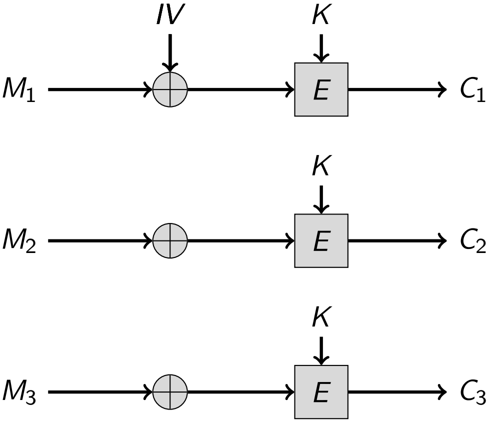


Image Credit: (Martin Thoma)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

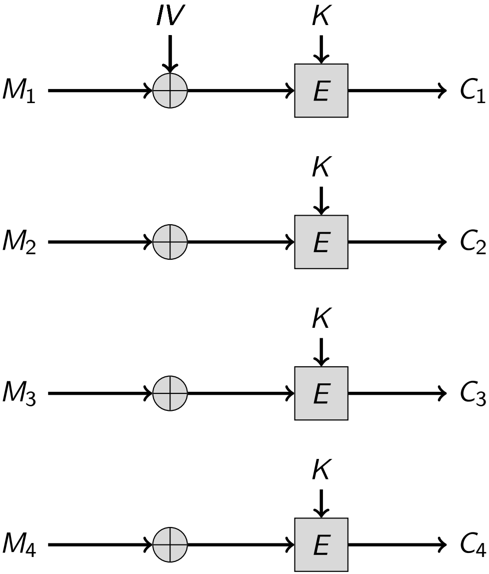


Image Credit: (Martin Thoma)

Cipher Block Chaining: CBC (not quite cryptocurrencies)

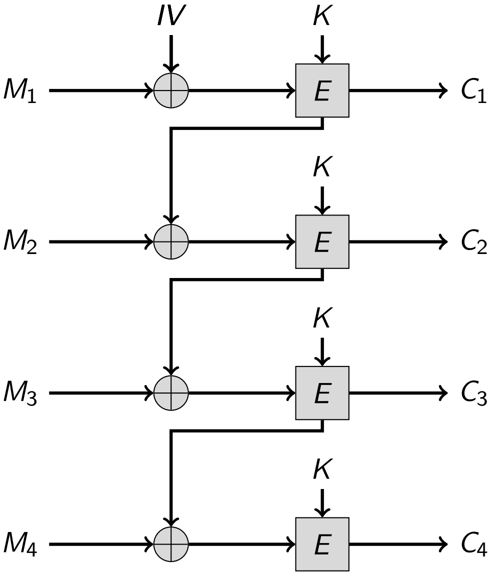


Image Credit (Martin Thoma)

CBC: Picking a good IV

CBC: Picking a good IV

- If you are developing a single use system, you do not even need an IV

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

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

Advanced Encryption System (AES)

Advanced Encryption System (AES)

- Developed by two belgian cryptographers, Joan Daemen and Vincent Rijmen

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

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

Advanced Encryption System (AES)

Advanced Encryption System (AES)

1. Derive round keys using key scheduler from cipher key

Advanced Encryption System (AES)

1. Derive round keys using key scheduler from cipher key
2. Expand the current key into the *round* key

Advanced Encryption System (AES)

1. Derive round keys using key scheduler from cipher key
2. Expand the current key into the *round* key
3. Complete encryption rounds

Advanced Encryption System (AES)

1. Derive round keys using key scheduler from cipher key
2. Expand the current key into the *round* key
3. Complete encryption rounds
    1. Non linear byte substitution according to look up table

Advanced Encryption System (AES)

1. Derive round keys using key scheduler from cipher key
2. Expand the current key into the *round* key
3. Complete encryption rounds
    1. Non linear byte substitution according to look up table
    2. Shift rows: last 3 rows are cyclically shifted

Advanced Encryption System (AES)

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

Advanced Encryption System (AES)

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

Advanced Encryption System (AES)

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

Advanced Encryption System (AES)

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

Advanced Encryption System (AES)

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

Advanced Encryption System (AES)

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