# Cryptography Notes

Samuel LaPree

September 21, 2023

## 1 2 Goals of Block Ciphers

There are 2 goals of block ciphers according to Shannon (founder of information theory)

- Confusion: The key and the ciphertext should be related in a complicated way. You can't "solve for the key" in some equation.
- Diffusion: Every bit of the ciphertext depends on every bit of plaintext
  - Small changes to plaintext $\longrightarrow\longrightarrow$ big change to ciphertext

Hill Ciphers have good diffusion but essentially no confusion

Modern ciphers achieve confusion using an S-Box (S stands for substitution)

## 2 S-Boxes

S-Box is a function that scrambles the input in a way that doesn't resemble any simple arithmetic function

S-Boxes are not secret

- Everyone uses the same S-Boxes
- S-Boxes never change

### 2.1 History of S-Boxes

In 1972 the NBS (National Bureau of Standards) now called NIST (National Institute of Standards and Technology), put out a call for proposals for a national encryption standard

IBM submitted a cipher called L.U.C.I.F.E.R.

The NSA made a bunch of changes

- Increased the number of rounds
- Changed the S-Boxes
- Added a weird permutation at the beginning

The result was called DES (Digital Encryption Standard) - the standard from 1970s - 1999

## 3 DES

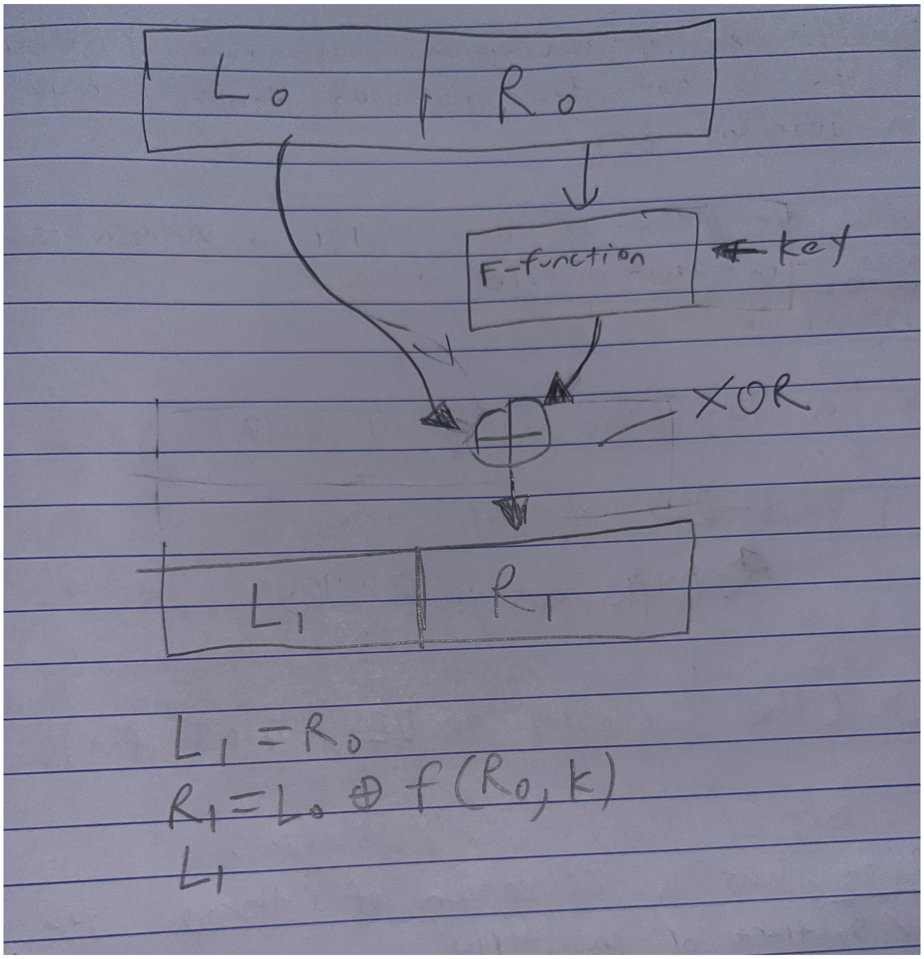
DES is based on a system called a feistel cipher

Idea: Bunch of rounds

Each round split block into 2 halves

| | |
|---|---|
| $L_0$ | $R_0$ |

### 3.1 Example




Encryption: Do this a bunch of times

Decryption: Swap of Left/Right. Do all rounds in reverse order.

### 3.2 DES Specifics

All the security rests on a good f-function

DES uses the following

- DES uses 16 rounds
- The blocksize is 64
- Key size is 56 bits
- Main flow of DES is "only $2^{56}$" keys

### 3.3 3-DES and AES

In DES double encryption with two different keys is not the same as single encryption with a different key

Double encryption of any cipher is vulnerable to a meet-in-the-middle attack

For a long time (up until 2017), 3-DES was still used
(Triple encryption DES)

AES which is the successor to DES uses finite fields

## 4 Rings

A Ring is a collection of things you can add/subtract or multiply

Examples:

- Integers - $\mathbb{Z}$
- Matrices

- Real numbers - $\mathbb{R}$
- Polynomials
- Rational numbers - $\mathbb{Q}$
- Complex Numbers - $\mathbb{C}$
- Residules (mod n) - $\mathbb{Z}_n$

A ring where every element other than 0 has an inverse is called a field.

# 5 Fields

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are all fields

A finite field is a field that is finite

$\mathbb{Z}_{26}$ is finite but not a field

For any integer n, there is at most 1 field having n elements

Write $\mathbb{F}$ or Gf(n) for the field with n elements

If p is prime, then every residue (mod p) has an inverse so

$$\mathbb{Z}_p = \mathbb{F}_p \text{ is a finite field}$$

If n is not prime (called composite) then,

$$\mathbb{Z}_n \neq \mathbb{F}_n \text{ (not a field!)}$$

AES uses $\mathbb{F}_{256}$ (not $\mathbb{Z}_{256}$)

### 5.1 Warm up

$\mathbb{F}_4 \neq \mathbb{Z}_4$

Write down addition/multiplication tables for $\mathbb{Z}_4$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

The row highlighted in blue shows that it is not a field

This is because $2x = 2$ has two solutions meaning we can't solve for $x$

Use polynomials

$\mathbb{F}_2[x] \leftarrow Ring$

All polynomials with coefficients in

$$\mathbb{F}_2[x] = \mathbb{Z}_2[x] = \{0, 1\}$$

### 5.2 Example

Let $f(x) = x^2 + 1$
$g(x) = x^2 + x + 1$ both be in $\mathbb{F}_2[x]$

What is $f(x) + g(x)$?

$$(\cancel{x^2} + \cancel{1}) + (\cancel{x^2} + x + \cancel{1}) = x$$

What is $f(x) * g(x)$?

$$= (x^2 + 1)(x^2 + x + 1)$$

$$= (x^4 + x^3 + \cancel{x^2})(\cancel{x^2} + x + 1)$$

$$= x^4 + x^3 + x + 1$$

Fun fact! : Euclid's Algorithm works in $\mathbb{F}_2[x]$