Confusion, Diffusion, DES & Finite Fields

There are 2 properties of modern ciphers (symmetric key), confusion, and diffusion...

Confusion:

The relationship between the ciphertext and the key should be complicated (so you can't just "solve" for the key using arithmetic)

Stream ciphers can have lots of confusion if the way to generate keystream is complicated), but have no diffusion.

Diffusion:

The relationship between the plaintext and the ciphertext should be complicated, if you change the plaintext a tiny bit the ciphertext should change in a big hard-to-predict way.

The hill cipher has lots of diffusion, but no confusion.

History

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

IBM (the International Business Machines Corporation) submitted a cipher they used, called L.U.C.I.F.E.R., and the NSA (National Security Agancy) made a bunch of changes to it, including:

- Adding more rounds
- Adding a permutation on the bits
- Changed the S-boxes

The result was called DES (Data Encryption Standard). DES was used by everyone from 1972 to the early 2000s, but in the late 90s people started to make computers fast enough to brute force DES by trying all 2^{56} keys.

Up until the late 2010s people still used Triple DES, which is just encrypting three times with DES using two keys k_1 and k_2

- $C = E_{k_1}(E_{k_2}(E_{k_1}(P)))$

DES

A symmetric-key algorithm with a relatively short key length of 56 bits. DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length.

In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt.

DES is largely depreciated, because even though it had 9 rounds, and the plaintexts were 64 bits, the master keys were only 56 bits long.

After DES was broken people used multiple keys encrypting multiple times with DES:

- Pick two keys k_1 and k_2
- Encrypt with both
  - $C = E_{k_2}(E_{k_1}(P))$
- Decrypt both sides:
  - $D_{k_2}(C) = E_{k_1}(P)$

It's important to know that double-encryption (with any cipher) is vulnerable to a meet-in-the-middle attack.

Fiestel Cipher

DES uses a recipe for ciphers called a Feistel Cipher, which takes two inputs – a data block and a subkey – and returns one output of the same size as the data block. In each round, the round function is run on half of the data to be encrypted, and its output is XORed with the other half of the data.

The basic idea of the Fiestel Cipher is to use lots of rounds, moving the left half L_i to the right R_i side.

- $R_{i+1} = L_i$
- $L_{i+1} = R_i \oplus f(L_i,\ k_i)$

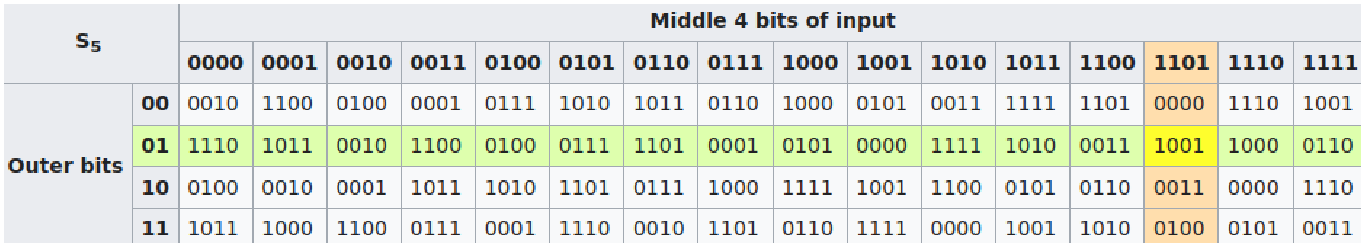
To specify a cipher using the Feistel recipe, you need to specify:

- How many rounds there are
- What $f(L,\ k)$ is
- How to produce round keys from the master key

S-Boxes

AKA Substitution Box, is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext by creating confusion.

Basically a big table that converts inputs to outputs in a permanent but seemingly random way.



S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Given a 6-bit input, the 4-bit output is found by selecting the row using the outer two bits (the first and last bits), and the column using the inner four bits. For example, an input "011011" has outer bits "01" and inner bits "1101"; the corresponding output would be "1001".

Finite Fields

Simply put, a field that contains a finite number of elements. Ring elements may be numbers such as integers or complex numbers, but they may also be non-numerical objects such as polynomials, square matrices, functions, and power series, all of which can have two binary operations satisfying properties analogous to those of addition and multiplication of integers (but not necessarily divide).

If every element of a ring (besides 0) has an inverse, we call it a field. Some examples of fields include:

- $\mathbb{R}$, real numbers
- $\mathbb{Q}$, rational numbers
- $\mathbb{C}$, complex numbers
    - $\mathbb{Z}$, integers is <u>NOT</u> a field
    - $\mathbb{Z}_n?$, no, but $\mathbb{Z}_p$ is if p is prime

We denote by $\mathbb{F}_n$ a field having n elements. There is at most one field having n elements for any integer n.

If p is prime, then $\mathbb{F}_p$ exists: $\mathbb{F}_p = \mathbb{Z}_p$ (integers $\mod p$). If n is not prime, then $\mathbb{F}_n \neq \mathbb{Z}_n$.

AES

Advanced Encryption Standard (which replaced DES) is a variant of the Rijndael block cipher

All the arithmetic in AES happens in $\mathbb{F}_{256} (\neq \mathbb{Z}_{256})$.

References

1. https://www.nist.gov/

2. https://www.britannica.com/topic/National-Institute-of-Standards-and-Technology
3. https://www.ibm.com/
4. https://www.britannica.com/topic/International-Business-Machines-Corporation
5. https://en.wikipedia.org/wiki/S-box
6. https://en.wikipedia.org/wiki/Data_Encryption_Standard
7. https://en.wikipedia.org/wiki/Feistel_cipher
8. https://en.wikipedia.org/wiki/Triple_DES
9. https://www.britannica.com/topic/Triple-DES
10. https://en.wikipedia.org/wiki/Meet-in-the-middle_attack
11. https://en.wikipedia.org/wiki/Finite_field
12. https://en.wikipedia.org/wiki/Ring_(mathematics)
13. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
14.

Links:

- 🧮 MATH 314 MOC

Created: 2024-02-21 14:08

#MATH314 #JuniorSemester2 #HigherEducation