2.1 Bitblock Ciphers—Introduction

Description

Bitblock ciphers operate over the alphabet $\Sigma = \mathbb{F}_2 = \{0,1\}$, and basically encrypt blocks of fixed length conserving this length, controlled by a key that itself is a bitblock of a certain length l. The encryption functions are defined as maps of the set $\mathbb{F}_2^n$ into itself, and the set $\mathbb{F}_2^l$ serves as key space.

For constructing and analyzing bitblock ciphers we usually view $\mathbb{F}_2^n$ as a vector space of dimension n over the two-element field $\mathbb{F}_2$. Sometimes we equip $\mathbb{F}_2^n$ with the structure of the field $\mathbb{F}_{2^n}$, on rare occasions we structure it as cyclic group of order 2^n, thinking of integer addition “with carry” $\bmod 2^n$.

Thus we describe a bitblock cipher as a map

$$F\colon \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$$

or as a family $(F_k)_{k\in K}$ of maps

$$F_k\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n \quad \text{for } k \in K = \mathbb{F}_2^l$$

where $F_k(a) = F(a,k)$.

Note In this chapter the mathematical symbol n is used for the length of the bitblocks, not for the size of the alphabet.

We might also view a bitblock cipher as a monoalphabetic substitution over the alphabet $\Sigma' = \mathbb{F}_2^n$.

The extension of a cipher to bitstrings of arbitrary lengths is subject of Chapter 3 on “modes”, and is of no concern for the moment, and likewise we don’t care how to pad shorter bitstrings.

Choice of the Block Length

The block length should be large enough to preclude the methods that break monoalphabetic substitutions, in particular analyses of patterns and frequencies. Moreover we would like to avoid any kind of leaks that reveal information about the plaintext, for example repeated ciphertext blocks.

If the sender didn’t systematically prevent repetitions, an attacker could mount a **codebook attack** by collecting pairs of ciphertext and known plaintext for a fixed (but unknown) key. In this way she would construct her own codebook. A large codebook would allow breaking many future messages even if it didn’t reveal the key. To prevent this attack we require:

- $\#\Sigma' = 2^n$ should be larger than the number of available memory cells, even assuming a very powerful attacker.

- Keys should be changed quite regularly.

In view of the Birthday Paradox an even stronger criterion is adequate: If the attacker has collected in her codebook about $\sqrt{\#\Sigma'} = 2^{n/2}$ plaintext-ciphertext pairs, the probability of a "collision" is approximately $\frac{1}{2}$. Therefore we require that the number $2^{n/2}$ surpasses the available storage. And keys should be changed long before this number of blocks is encrypted.

In the "pre-AES" age bitblock ciphers usually had 64-bit blocks. From our point of view this is by far insufficient, at best justified by frequent key changes. We prefer 128 bits as block length. This is also the block length of the new standard AES.

This consideration might look somewhat paranoid. But it is a typical example of the security measures in modern cryptography: The cipher designers work with large security margins and avoid any weaknesses even far away from a practical use by an attacker. Thus the security requirements of modern cryptography by far surpass the requirements typical for classical cryptography. This may sound exaggerated. But the modern algorithms—that in fact offer these huge security margins—can also resist future progress of cryptanalytic capabilities.