DES and AES

I would like to end this section with a brief description of some modern symmetric cryptosystems that are actually used in commercial applications rather than the toy examples I have discussed so far.

The data encryption standard (DES) was adopted in the US in 1977, and it became the most widely used encryption scheme until its replacement in 2001 by the advanced encryption standard (AES).

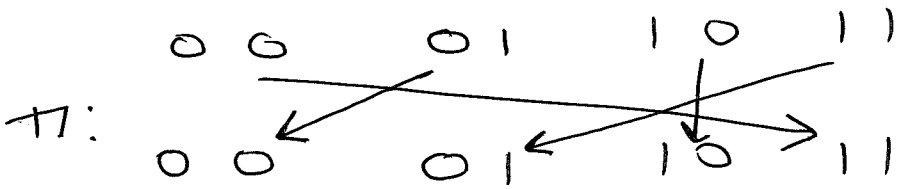
DES (I shall not discuss AES here) is a block cipher in which data is encrypted in blocks 64 bits long (i.e. should be regarded as elements of $\mathbb{Z}_2^{64}$) using a key 56 bits long.

I am going to sketch out the ideas behind DES although I won't give all the details which are more technical than mathematical. You can find out more about DES and AES in Stallings' book. I recommend "Simplified DES" invented by Edward Schaefer and which can be found described on the web.

A block cipher is one in which the plaintext is divided into blocks of strings each of the same fixed length n. For example, in DES $n = 64$.

If A is an alphabet then A^n is the set of all strings of length n over A. Thus the most general block cipher is a bijection $\pi : A^n \to A^n$.

Example $A = \mathbb{Z}_2$, $n = 2$.



Cleartext: 001011

Ciphertext: 111001

The total no. of blockciphers = no. of perms of the set A^n

$= |A|^n!$ ∴ if $A = \mathbb{Z}_2$, then the no. of binary block ciphers is $(2^n)!$

How do we describe a block cipher?
Choose and fix an ordering of the elements in A^n;
then list where each block is sent to. There are
$|A|^n$ blocks and each block has size n.
Thus $n|A|^n$ symbols are needed to describe
the block cipher.

Example Our cipher above could be described by

$$(11, 00, 10, 01)$$

which contains $2 \cdot 2^2 = 8$ bits.

Thus a binary block cipher with block size 64
would need $64 \cdot 2^{64}$ bits in order to be
described. This is also the length of the key.
This is a tad large.

Thus to design a practical block cipher we need to bear in mind the following points:

- if we have small block size then the system will be vulnerable to the statistical approaches that I have hinted at earlier.

- But an arbitrary block cipher is not practical because of the huge keysize needed.

- However, the key should not be so small that the cipher is susceptible to an exhaustive search.

- We have seen that the cipher should not be affine because it can be broken by a known plaintext attack.

Horst Feistel, Cryptography and Computer privacy, Scientific American, May, 1973.

How do we construct a symmetric block cipher that satisfies these constraints and is secure. I shall now describe some of the ideas that lie behind DES and are due to Horst Feistel:

Idea 1 How to build a bijective function from an arbitrary function.

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be <u>any</u> function. In particular, f is not necessarily bijective and ultimately is <u>not</u> linear.

We shall use f to construct a bijective function $\varphi : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^{2n}$.

[We write elements in $\mathbb{Z}_2^{2n}$ in the form $(\underline{x}, y)$ where $\underline{x}, y \in \mathbb{Z}_2^n$]

Define $\varphi(\underline{x}, y) = (\underline{x}, y + f(\underline{x}))$

Claim φ is bijective. It is enough to show that φ is injective.

Suppose that $\varphi(\underline{x}_1, y_1) = \varphi(\underline{x}_2, y_2)$.

Then $(\underline{x}_1, y_1 + f(\underline{x}_1)) = (\underline{x}_2, y_2 + f(\underline{x}_2))$.

Then $\underline{x}_1 = \underline{x}_2$ and $y_1 + f(\underline{x}_1) = y_2 + f(\underline{x}_2)$.

$\therefore f(\underline{x}_1) = f(\underline{x}_2)$ and so $y_1 = y_2$.

[We use the fact that $(\mathbb{Z}_2, +)$ is a group]

Idea 2 The swap function

$$(x, y) \xrightarrow[\sigma]{\text{swap}} (y, x).$$

Idea 3 Iteration

Let $f_1, f_2 : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ be arbitrary.

Define $\varphi_1(x, y) = (x, y + f_1(x))$

$\varphi_2(x, y) = (x, y + f_2(x))$

Input (x, y)

σ

(y, x)

do φ_1

$(y, x + f_1(y))$

} round 1

σ

$(x + f_1(y), y)$

do φ_2

$(x + f_1(y), y + f_2(x + f_1(y)))$

} round 2

if f_2 "nasty" then no simplification is possible here.

Idea 4 Rather than having separate functions $f_1, f_2, \ldots, f_s : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ have <u>one</u> function $F : \mathbb{Z}_2^k \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. For each choice of $\underline{k} \in \mathbb{Z}_2^k$, we have that $F(\underline{k}, -) : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, which can represent f_i

Idea 5 Idea behind DES. Choose $F : \mathbb{Z}_2^k \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ suitably nasty. This is fixed and forms the architecture of the cryptosystem. Choose a key $\underline{K}$.

- From $\underline{K}$ construct subkeys $\underline{k}_1, \ldots, \underline{k}_s$ in a fixed way.
- Define $f_i = F(\underline{k}_i, -)$. <u>Idea 4</u>
- Define φ_i from f_i. <u>Idea 1</u>
- Cleartext $= (\underline{x}, \underline{y})$

  Ciphertext = <u>Ideas 2 and 3</u>

$$(\varphi_s \sigma)(\varphi_{s-1} \sigma) \cdots (\varphi_1 \sigma)(\underline{x}, \underline{y})$$

s is "large" such as $s = 16$.

Idea 6 $F: \mathbb{Z}_2^k \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$

is "nasty" if it can be made to depend on a problem that is known, or strongly suspected, of being intractable.

DES is based on the following problem that is known to be "nasty":

> Given polynomials $P_1, \ldots, P_m$ in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}_2$. Do these polynomials have a common zero?

This helps to defeat the problem that did for affine block ciphers — it makes the cryptosystem more resistent to known plaintext attacks.