Example 134. (DES-X) To increase the key size of DES, the following variation, known as DES-X, was proposed by Ron Rivest in 1984:

$$c = k_3 \oplus \mathrm{DES}_{k_2}(m \oplus k_1)$$

What is the key size of DES-X? What about the effective key size?

Solution. k_1 and k_3 must be 64 bit, while k_2 is 56 bits. That's a total key size of 184 bits for DES-X.
However, just like for 3DES, the possibility of a meet-in-the-middle-attack reduces the effective key size to at most $184 - 64 = 120$ bits.
Comment. This approach of xoring with a subkey before and after everything else is known as **key whitening**. This features in many modern ciphers, including AES.

Example 135. (bonus!) Using DES, are there blocks m, c such that $E_k(m) = c$ for more than one key k?

I don't know the answer and couldn't find it easily. Maybe you are more skilled?

To construct the finite field $\mathrm{GF}(p^n)$ of p^n elements, we can do the following:

- Fix a polynomial $m(x)$ of degree n, which cannot be factored modulo p.
- The elements of $\mathrm{GF}(p^n)$ are polynomials modulo $m(x)$ modulo p.

Irreducible mod p? A polynomial is irreducible modulo p if and only if it cannot be factored modulo p.
For instance, the polynomial $x^2 + 2x + 1$ can always be factored as $(x+1)^2$.
For the polynomials $m(x) = x^2 + x + 1$ things are more interesting:

- $x^2 + x + 1$ cannot be factored over $\mathbb{Q}$ because the roots $\frac{-1 \pm \sqrt{-3}}{2}$ are not rational.
- However, $x^2 + x + 1 \equiv (x+2)^2$ modulo 3, so it can be factored modulo 3.
- On the other hand, $x^2 + x + 1$ is irreducible modulo 2 (that is, it cannot be factored: the only linear factors are x and $x+1$, but x^2, $x(x+1)$ and $(x+1)^2$ are all different from $x^2 + x + 1$ modulo 2).

Comment. Actually, all finite fields can be constructed in this fashion. Moreover, choosing different $m(x)$ to construct $\mathrm{GF}(p^n)$ does not matter: the resulting fields are always isomorphic (i.e. work in the same way, although the elements are represented differently). That justifies writing down $\mathrm{GF}(p^n)$, since there is exactly one such field.

Example 136. AES is based on representing bytes as elements of the field $\mathrm{GF}(2^8)$. It is constructed using the polynomial $x^8 + x^4 + x^3 + x + 1$ (which is indeed irreducible mod 2).

Example 137. As seen above, the polynomial $x^2 + x + 1$ is irreducible modulo 2, so we can use it to construct the finite field $\mathrm{GF}(2^2)$ with 4 elements.

(a) List all 4 elements, and make an addition table. Then realize that this is just xor.

(b) Make a multiplication table.

(c) What is the inverse of $x + 1$?

Armin Straub
straub@southalabama.edu

Solution.

(a) The four elements are $0, 1, x, x+1$.
For instance, $(x+1)+x = 2x+1 = 1$ (in $\mathrm{GF}(2^2)$, since we are working modulo 2). The full table is below.
Each of the four elements is of the form $ax+b$, which can be represented using the two bits ab (for instance, $(10)_2$ represents x and $(11)_2$ represents $x+1$).
Then, addition of elements $ax+b$ in $\mathrm{GF}(2^2)$ works in the same way as xoring bits ab.

(b) For instance, $(x+1)^2 = x^2+2x+1 \equiv x^2+1 \equiv x$.
The key to realize is that reducing modulo x^2+x+1 is the same as saying that $x^2 = -x-1$, i.e. $x^2 = x+1$ in $\mathrm{GF}(2^2)$. That means all polynomials of degree 2 and higher can be reduced to polynomials of degree less than 2.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

(c) We are looking for an element y such that $y(x+1) = 1$ in $\mathrm{GF}(2^2)$. Looking at the table, we see that $y = x$ has that property. Hence, $(x+1)^{-1} = x$ in $\mathrm{GF}(2^2)$.

Example 138. (homework) The polynomial x^3+x+1 is irreducible modulo 2, so we can use it to construct the finite field $\mathrm{GF}(2^3)$ with 8 elements.

(a) List all 8 elements, and multiply all of them with $x+1$.

(b) What is the inverse of $x+1$?

Solution.

(a) The elements are $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$.
[Note that $x^3 = -x-1 = x+1$ in $\mathrm{GF}(2^3)$. That means all polynomials of degree 3 and higher can be reduced to polynomials of degree less than 3.]
When multiplying, we calculate, for instance: $(x+1)x^2 = x^3+x^2 = x^2+x+1$
Similarly: $(x+1)(x^2+1) = (x+1)x^2+(x+1) \equiv (x^2+x+1)+(x+1) \equiv x^2$
Or: $(x+1)(x^2+x) = (x+1)x^2+(x+1)x \equiv (x^2+x+1)+(x^2+x) \equiv 1$

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x

(b) We are looking for an element y such that $y(x+1) = 1$ in $\mathrm{GF}(2^3)$. Looking at the table, we see that $y = x^2+x$ has that property. Hence, $(x+1)^{-1} = x^2+x$ in $\mathrm{GF}(2^3)$.

5.2 Basics of AES

The block cipher AES (short for **advanced encryption standard**) replaced DES. By now, it is the most important symmetric block cipher.

1997: NIST requests proposals for AES (receives 15 submissions) [very different from how DES was selected!]
2000: Rijndael (by Joan Daemen and Vincent Rijmen) selected (from 5 finalists)
[AES-192/256 is first (and only) public cipher allowed by NSA for top secret information.]

- 128 bit block size (as per NIST request)
- key size 128/192/256 bit (10, 12, 14 rounds)