Review

We studied the basic algorithm for DES, and its extension to triple DES. The main point of the in-class discussion was, in fact, the main point of the initial debate over DES: the contents of the $S$-boxes. Recall that the $S$-boxes enable us to compute the inner round function $f$ by table lookup. The row and column are functions of the input and the round key, so both have an effect. Variations on DES include changing the $S$-boxes, but it is possible to choose $S$-boxes, or round functions, that do not obscure the patterns in the original data.

We also briefly discussed key distribution, a topic we will discuss in more detail later. If you are sending data over an insecure channel (this includes the internet, cell phones, or shouting across the room), then sending the key along that channel means that it is subject to intercept. Once an opponent has the key, you have no security. It is tempting to choose DES keys that are easy to communicate; this usually means ASCII text. But this significantly reduces the size of the key space that an opponent might search.

Introduction

Part of the controversy about the contents of the $S$-boxes is that their design criteria were not made public. DES has been replaced by the Advanced Encryption Standard (AES), which was chosen by the US National Institute of Standards and Technology (NIST) after an extensive public competition. NIST’s choice of Rijndael was partly influenced because the algorithm is easy to analyze. Everything about it is transparent. The idea is that a transparent system is that any weakness will be easier to find, because you know exactly what each part of the algorithm is supposed to do.

The difficulty is in the definition of “easy:” compared to what? The ease of analysis of Rijndael depends on the fact that all of the operations are expressed in arithmetic over a finite field. This was once one of the obscure areas of abstract algebra, but has now been thrust into the mainstream of applications.

So we will study arithmetic over finite fields. In fact, you have probably already studied this, a little, when you studied the Greatest Common Divisor algorithm.

Groups

A group is an algebraic system consisting of a set $G$ with an operation $\cdot$ that satisfies a small number of axioms:

- [Associative Property] For all $x_i \in G$, $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$
• [Existence of an Identity] There is an element \( e \in G \) such that for all \( x \), \( e \cdot x = x \cdot e = x \).

• [Existence of Inverses] For every element \( x \) there is an element \( y \) such that \( xy = e \).

[Various authors play games with equivalent formulations of these axioms, but that is a subject for a different course.]

The primary example of a group is the group of integers under addition. This group also has the property that \( x + y = y + x \) for all elements, which makes it abelian. We will only talk about abelian groups, and will denote the operation by the familiar symbol of horizontal and vertical line segments joined at their midpoints, or \(+\).

The most important groups for us are the groups \( \mathbb{Z}/n\mathbb{Z} \), consisting of the integers 0 through \( n - 1 \) with addition modulo \( n \). Thus, in \( \mathbb{Z}/7\mathbb{Z} \), \( 4 + 5 = 2 \), because \( 9 \mod 7 = 2 \).

---

**Rings**

A ring is a group with another operation, called multiplication, and denoted by concatenation. The two operations must be compatible in the sense that the usual distributive laws

\[
\begin{align*}
a(b + c) &= ab + ac \\
(a + b)c &= ac + bc
\end{align*}
\]

for all \( a, b, \) and \( c \).

All of our rings will have an identity element \( 1 \) for multiplication, and we use \( 0 \) for the additive identity.

The sets \( \mathbb{Z}/n\mathbb{Z} \), with operation modulo \( n \), form rings. In \( \mathbb{Z}/7\mathbb{Z} \), \( 4 \cdot 5 = 6 \). Notice that some of these rings can have zero-divisors, that is, nonzero elements whose product is \( 0 \). For example, in \( \mathbb{Z}/12\mathbb{Z} \), \( 3 \cdot 4 = 0 \). An element with an inverse is called a unit. In \( \mathbb{Z}/12\mathbb{Z} \), \( 5 \) is a unit, because \( 5 \cdot 5 = 25 \equiv 1(12) \). A ring without zero divisors is called an integral domain.

---

**Fields**

A field is a ring in which every element, except \( 0 \), has an inverse. The rings \( \mathbb{Z}/p\mathbb{Z} \), with \( p \) prime, are fields. It is a theorem that the cardinality of every finite field is a power of a prime. Rijndael uses the field with \( 256 = 2^8 \) elements.

Construction of the prime fields is straightforward: use \( \mathbb{Z}/p\mathbb{Z} \). The others require some work, however. Notice that \( \mathbb{Z}/4\mathbb{Z} \), which has \( 4 \) elements, is not a field, because \( 2 \cdot 2 = 0 \), meaning that \( 2 \) has no inverse.

---

**Polynomials**

The key tool in constructing and understanding fields of prime power order is the polynomial. Remember that a polynomial is an expression of the form \( a_nx^n + \cdots + a_0 \), where
$x$ is an indeterminate, and the coefficients $a_j$ come from the field of definition. The set of all polynomials with coefficients in a fixed field $k$ forms a ring (maybe one should say this forms the ring) denoted $k[x]$. The addition and multiplication are the same that you learned in high school algebra.

For example, let $k = GF(2)$, the field of order two, whose elements are $\{0,1\}$. Typical polynomials are $p(x) = x^2 + x + 1$ and $q(x) = x^3 + x + 1$. The sum $p + q$ is $x^3 + x^2$; the $x$ coefficient is $1 + 1 = 0$, as is the $x^0$ coefficient. Their product is

$$ (x^3 + x + 1)(x^2 + x + 1) = (x^5 + x^4 + x^3) + (x^3 + x^2 + x) + (x^2 + x + 1) = x^5 + x^4 + 1. $$

---

**Algorithms**

The basic algorithm for operation in “good” rings is the Euclidean algorithm. Over the integers, this says that given $n$ and $m$ there are unique integers $q$ and $r$, with $r < n$, such that $m = qn + r$. Usually $q$ is called the quotient and $r$ is the remainder. For example, if $m = 16$ and $n = 5$, we have $16 = 5 \cdot 3 + 1$, so $q = 3$ and $r = 1$.

This is the basis of the GCD algorithm that you have probably studied. This usually is based on the recursion operation $\gcd(a, b) = \gcd(b, a \mod b)$. For example, to find the GCD of 56 and 22, note that

$$ \gcd(56, 22) = \gcd(22, 12) \quad \text{since } 56 \mod 22 = 12 $$
$$ = \gcd(12, 10) \quad \text{since } 22 \mod 12 = 10 $$
$$ = \gcd(10, 2) $$
$$ = 2. $$

The reason this works is as follows. Suppose that $a = qb + r$, and that $d$ is a common divisor of $a$ and $b$. Then $d$ divides $a - qb$, so it divides $r$, and is thus a common divisor of $b$ and $r$. Reverse this to see that a larger common divisor of $r$ and $b$ must also divide $a$.

If $d = \gcd(a, b)$, then one can find $x$ and $y$ such that $ax + by = d$. The quickest proof is not very quick: it depends on ring theory. But we can extend the Euclidean algorithm to find $x$ and $y$ for us, which is a pretty good proof. The trick is to write $a = a \cdot 1 + b \cdot 0$, and $b = a \cdot 0 + b \cdot 1$. Now, perform the Euclidean algorithm on $a$ and $b$ in both forms, simultaneously. In the example above, $56 = 56 \cdot 1 + 22 \cdot 0$, and $22 = 56 \cdot 0 + 22 \cdot 1$. The GCD of 56 and 22 is the GCD of 22 and 12, where $12 = 56 - 2 \cdot 22$. Simultaneously,

$$ 56 - 2 \cdot 22 = 56 \cdot 1 + 22 \cdot 0 - 2 \cdot (56 \cdot 0 + 22 \cdot 1) $$
$$ = 56 \cdot (1 - 2 \cdot 0) + 22 \cdot (0 - 2 \cdot 1) $$
$$ = 56 \cdot 1 + 22 \cdot (-2). $$

Now, we are trying to find the GCD of 22 and 12 = 56 \cdot 1 + 22 \cdot (-2); this is the GCD of 12 and 10 = 22 - 12, which is

3
The key entries here are the coefficients of 56 and 22 in each expression, so we extend the Euclidean algorithm to operate on triples. We start with $(1, 0, 56)$ and $(0, 1, 22)$. The next pair of triples is $(0, 1, 22)$ and $(1, -2, 12)$. Next is $(1, -2, 12)$ and $(-1, 3, 10)$. We keep going until the last term is $(x, y, d)$. At every stage of the algorithm $(a, b, c)$ means that $a \cdot 56 + b \cdot 22 = c$, so we are done.

The Euclidean algorithm works in polynomial rings like $GF(p^l)[x]$, using degree in place of less than; that is $m(x) = n(x)q(x) + r(x)$, where the degree of $r$ is less than the degree of $n$. 

$56 \cdot (-1) + 22 \cdot 3$ [try it!].