Computer Science Tripos part 2 – Security

Lecture 9 – Factorisation

This lecture will be given by a guest speaker, Paul Leyland from Microsoft Research. Paul was one of the team that factored RSA 129, a 129-digit product of two primes which was set as a challenge by Rivest, Shamir and Adleman following the discovery of the cryptosystem named after them.

I append a paper by Peter Montgomery which gives worked examples of many of the factoring techniques which will be discussed.

For those who did not do maths as an option in part 1a, I will revise some terminology. The words 'group', 'ring' and 'field' are used often in papers on public key cryptology so it is important to understand what they mean (we do not need any deep results). Mathematicians use these concepts to generalise and refine our intuition about arithmetical operations.

A *group* is a set with an operation which is associative (i.e., $a(bc) = (ab)c$), has an identity ($a.1 = 1.a = 1$) and where each element has an inverse (for each a there is an a^{-1} such that $a.a^{-1} = a^{-1}.a = 1$). If a group has n elements, we say it is of order n, while the order of a group element, $\mathrm{ord}(a)$, is the smallest positive integer k such that $a^k = 1$.

The obvious examples of groups are the non-zero rational numbers under multiplication, and the whole numbers under addition (in which case, the identity is of course 0). However, groups do not need to have $ab = ba$; examples of groups for which ab and ba are in general different include multiplication of matrices and permutations on a set of objects (An example of a permutation is (1342) which permutes the four objects ABCD to ACDB; the group operation is composition. The group whose $n!$ elements are the permutations on n objects is called the symmetric group on n letters, written Σ_n; a random permutation in the sense of a k-bit block cipher is just a randomly chosen element of Σ_{2^k}).

An *Abelian group* is a group whose operation is commutative, i.e. $ab = ba$ holds for all a and b. Examples of Abelian groups include the whole numbers modulo any positive integer n under addition, and the nonzero whole numbers modulo any prime p under multiplication.

A *ring* is a generalisation of the whole numbers; it is a set with two operations – $+$ and $.$ – such that the elements form an Abelian group under $+$, while $.$ acts on nonzero elements and is associative, and the distributive law holds ($a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$). The important example for cryptography is the ring of polynomials, and especially polynomials whose coefficients take the values 0 and 1.

A *field* is a generalisation of the rational numbers or the real numbers; it is a ring in which the nonzero elements form an Abelian group under the multiply operation, and thus almost all our intuitions about rational number arithmetic can be carried over. The important examples for cryptography are the finite fields. The field with p elements can be constructed as the integers modulo p.

Just as we construct the complex numbers from the real numbers by adding the symbol 'i' to denote a root of the equation $x^2+1=0$, so also we can construct a field with p^2 elements from the field with p elements by adding a root of a polynomial which is irreducible (has no proper factors). One can prove that all polynomial equations are soluble in the complex numbers; the comparable theorem for finite fields says that if we make a field with p^k elements by adjoining a root of an irreducible polynomial of degree k, then all polynomials of degree up to and including k are fully soluble. A consequence of this is that there is essentially only one field of order p^k for every prime p and positive integer k (given a field generated by adjoining a root of any other equation, we can use the solution of that equation in the first field to construct an isomorphism between the two fields).

An alternative construction of the finite field of order p^k is to take the ring of polynomials over the field of p elements, modulo an irreducible polynomial of degree k. There is also a relationship with shift registers, in that successive states of a shift register of length k can be seen as successive powers of an element of the finite field with 2^k elements. For the details of all this, see Lidl and Niederreiter's *'Finite Fields'*; there is a more concise treatment of the basics in Lang's *'Algebra'*.

The only other results that we will mention are that if a group has order n, then all its subgroups will have orders dividing n (Lagrange's theorem); and that such subgroups will exist for all of the proper factors of n (Sylow's first theorem).

Problems

1. Prove that every element in a finite group has finite order.
2. Prove Lagrange's theorem.
3. Prove Sylow's first theorem for finite Abelian groups, and then for general finite groups.
4. In 1873, William Jevons speculated that no-one would ever know the factors of 8,616,460,799 other than himself. Factor this number using (at most) a calculator, and estimate how long it would take with pencil and paper.
5. Hardy and Wright's *'The Theory of Numbers'* reports that $\pi(10^9)$ – the number of prime numbers less than one billion – is 50,847,478. Is this correct?