Conclusions

As a result of these and other changes, enrolment in the honours Mathematics programs began to increase sharply in recent years, and the first year numbers are now three times their previous levels. Although there are other factors at work here, the introduction of symbolic computation in first year has certainly contributed to this development. There is a noticeable improvement in the attitude of the students to Mathematics. The computer is clearly acting as a bridge for them into an area that they otherwise would not feel they could reach.

Finally, the Mathematics courses themselves are changing, and the use of software such as MAPLE is driving this change. New types of problems are now accessible which could not be tackled by hand. Some parts of our courses have become obsolete, and must be ruthlessly pruned. New branches of Mathematics are emerging. The long-term effect of this will be interesting to see. One thing is clear: if we are not preceived by our students as leading in this revolution rather than being dragged along, then Mathematics will, by the turn of the century, be a neglected backwater.

NOTES

A public key cryptosystem as hard as factorisation

M. Christopher W. Jones

1 Introduction

The idea of a public-key cryptosystem was first put forward by Diffie & Hellman in their 1976 paper [7]. Since then various descriptions of it have appeared [3,11,14,24,27] including a recent Bulletin article [10]. The idea behind a public-key cryptosystem is that it allows secret messages to be sent across an open channel without it being necessary for some additional piece of information to be previously exchanged between sender and receiver.

Briefly, the idea is this. If Mr. X wishes to receive secret communications he constructs an *encryption function* E and a *decryption function* D. These should possess the following properties: (i) $D(E(m)) = m$ for all messages m, (ii) both E and D should be easily computable, (iii) it should not be possible to determine D from a knowledge of E alone, (iv) $E(D(m)) = m$ for all messages m. (Actually property (iv) is not absolutely essential, but is useful for purposes of authentication - for more details consult the above references.)

Mr. X then publishes the encryption function E (the *public key*) and keeps the decryption function D to himself (the *secret key*). Anyone wishing to send him a message m then transmits the encrypted message $E(m)$. On receiving this, Mr. X is able to recover the original message using D and property (i). However any eavesdropper who intercepts $E(m)$ is unable, because of property (iii), to discover m, even if he knows the encryption function E.

In order to put the above scheme into practice it is necessary to construct suitable encryption/decryption functions. One way this has been attempted is by the use of a "trapdoor" function f: this is a function for which it is easy to compute $f(x)$ but very difficult to compute $f^{-1}(x)$ without some additional

"trapdoor" information. However with the knowledge of the "trapdoor" information $f^{-1}(x)$ should be easy to compute.

Most attempts to construct "trapdoor" functions consist of putting some computationally hard problem between f and f^{-1}. Then to quote from [10], "... solving the hard problem implies breaking the cryptosystem and *it is hoped* that ... the cryptosystem cannot be broken *without* solving the hard problem. In no case has this been proved ..."

It is the purpose of this note to describe a cryptosystem, due to Rabin [16], which has the property that breaking it *is* equivalent to solving a computationally hard problem, specifically that of integer factorisation. In this respect, Rabin's scheme bears certain similarities to the well-known RSA scheme [10,20,27]. However Rabin's scheme possesses the important difference that breaking it is known to be *equivalent* to factorising an integer; whereas in the case of the RSA scheme, all that is known is that no-one has yet been able to devise a method of breaking it which does not involve factorisation.

The problem of factorisation of large integers has received much attention in the last twenty years, ever since the use of computers became commonplace. At present the most efficient algorithms for factorising a number n have average running times of order $\exp(\log n \log\log n)^{1/2}$ (see [8,9,26]). Riesel [18,19] states that the present upper limit for factorisation is 10^{75} and he estimates that with the most sophisticated technology available, factorisation of a hundred digit number would take one year. However, it may be noted that few theoretical results above the difficulty of factorisation are known - it is not, for instance, known whether the factorisation problem is NP-hard (see [12,23,27]).

To conclude, perhaps we should note that the *factorisation* problem should not be confused with the *primality* problem which is to determine whether a given integer is prime or not. This problem is much easier and there are algorithms ([2,5,9,15,17,25]) by means of which a computer can determine the primality of a 200 digit number in ten minutes. Indeed, as we shall see, in order to implement the Rabin cryptosystem it is essential that we can easily generate large (say 100 digit) primes. In passing, readers might be interested to learn that a new largest known prime has recently been discovered. The largest known prime is now $391581 \times 2^{216193} - 1$, and was discovered by a group working in the Amdahl Corporation, Sunnyvale, California [4,6]. (This compares with the previous largest known prime which was $2^{216091} - 1$, a record which has stood since 1985.)

2 Number Theoretic Preliminaries

In this section we give a brief account of the number theory necessary for a description of Rabin's method. For proofs of the results stated, see almost any book on number theory, for instance [13,21,22].

Let n be a positive integer greater than 1 and let y be an integer which is non-zero (mod n). Then if the congruence $x^2 \equiv y \pmod{n}$ is soluble, y is said to be a *quadratic residue* (mod n). Given y and n, it is straightforward to discover whether or not y is a quadratic residue (mod n) by means of the celebrated *law of quadratic reciprocity*. Now suppose $n = p$, an odd prime. Then exactly half of the non-zero integers (mod p) are quadratic residues in which case the congruence $x^2 \equiv y \pmod{p}$ has precisely two incongruent (mod p) solutions which may be written x_0 and $p - x_0$. In the special case when p is of the form $4k + 3$, we have the result that $x_0 \equiv y^{\frac{p+1}{4}} \pmod{p}$. (This follows from *Euler's criterion* which states that y is a quadratic residue (mod p) if and only if $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.)

In the case when $n = pq$, a product of two primes, it may be shown that y is a quadratic residue (mod n) if and only if y is a quadratic residue (mod p) *and* y is a quadratic residue (mod q). When this is true, and in the particular case when p and q both have the form $4k + 3$, there is a straightforward procedure for solving $x^2 \equiv y \pmod{n}$ (*provided* the factorisation of n is known).

To find the solutions, first determine integers a and b such that $ap - bq = 1$. (Such integers must exist because the greatest common divisor of p and q is 1 and they can easily be found by the Euclidean algorithm.) Now denote the solutions of $x^2 \equiv y \pmod{p}$ by u and $p - u$ and the solutions of $x^2 \equiv y \pmod{q}$ by v and $q - v$. Then it is a routine calculation to verify that the four solutions of the original congruence are

$$x_1 = bqu + apv, \quad x_2 = bq(p - u) + apv,$$

$$x_3 = bq(p - u) + ap(q - v), \quad x_4 = bqu + ap(q - v).$$

These four solutions are clearly incongruent (mod n) and it is not hard to show that they are the only solutions (mod n) of $x^2 \equiv y \pmod{n}$.

We may now give a description of the Rabin cryptosystem, the security of which depends essentially on the fact that solving $x^2 \equiv y \pmod{n}$ is *equivalent* to factorising n.

3 The Rabin Cryptosystem

A user of the Rabin system who wishes to receive messages first picks two primes p and q both of which are of the form $4k+3$. He also picks a positive integer $a < n = pq$. Then the integers n and a are made public while the primes p and q are kept secret. In order to encrypt a message m, which must be an integer between 0 and $n-1$, a sender calculates

$$E(m) = m(m+a) \pmod{n}.$$

If the resulting encrypted message is e, the receiver, who knows the factorisation of n, can easily decipher it by means of the following procedure:

It is required to find m which satisfies

$$m^2 + am \equiv e \pmod{n}.$$

Multiplying through by 4 this becomes

$$4m^2 + 4am \equiv 4e \pmod{n},$$

which may be written

$$(2m+a)^2 \equiv 4e + a^2 \pmod{n}.$$

Now, since the factorisation of n is known, it is straightforward to solve $x^2 \equiv 4e + a^2 \pmod{n}$ by means of the method outlined in §2. When this has been done m may be determined by solving the linear congruence $2m \equiv x - a \pmod{n}$. Note that there will be, in general, four values of x and hence four possible messages m. This illustrates a weakness of the Rabin scheme in that the deciphering process does not lead back to a unique value of m. However, assuming the original message was written in English, it will normally be obvious which of the different possibilities for m is the correct one.

(It may be noted here that property (iv) of the list given in §1, that $E(D(m)) = m$ for all messsages m, does hold in the Rabin system, whichever value is taken for $D(m)$.)

It is clear from the description given above that breaking the Rabin system cannot be *harder* than factorisation. To show that it is in fact equivalent it will be sufficient to show that if there were an efficient algorithm for solving $x^2 \equiv y \pmod{n}$, where $n = pq$, then it would be possible to factorise n. To

see that this is indeed so, suppose that it were possible to solve $x^2 \equiv y \pmod{n}$. Then by §2 the solutions are:

$$x_1 = bqu + apv, \qquad x_2 = bq(p-u) + apv,$$
$$x_3 = bq(p-u) + ap(q-v), \qquad x_4 = bqu + ap(q-v).$$

(Note that $x_1 \equiv -x_3 \pmod{n}$ and $x_2 \equiv -x_4 \pmod{n}$.) Then $x_1 + x_2 = p(bq + 2av)$ and so p is the greatest common divisor of $x_1 + x_2$ and n. Since g.c.d.'s can be found easily using the Euclidean algorithm, this factorises n.

Rabin's original cryptosystem was rather more sophisticated than the simplified version given here. He relaxed the condition that p and q have the form $4k+3$. This means that another more complicated method, due to Adleman *et al*, for solving quadratic congruences has to be used. For more details see [1,15,16].

4 An example

We illustrate this system with an example. Let $p = 59, q = 47, n = 2773$ and $a = 1371$. Now suppose we wish to send the message

TRINITY COLLEGE

The first step is to convert this into numerical form using the scheme $A = 00, B = 01 \ldots Z = 25$, space $= 26$. The message then becomes, divided into blocks of four,

1917 0813 0819 2426 0214 1111 0406 0426.

To encipher the first block, we calculate

$$E(1917) = 1917(1917 + 1371) \equiv 0067 \pmod{2773}.$$

In this way the whole message enciphers as

0067 0872 2252 2389 0884 1140 0482 0174.

To decipher this, it is required to find m such that

$$m^2 + 1371m \equiv 0067 \pmod{2773}.$$

Completing the square this becomes

$$(2m + 1371)^2 \equiv 2588 \pmod{2773}.$$

The next step is to solve $u^2 \equiv 2588 \pmod{59}$, which simplifies to $u^2 \equiv 51 \pmod{59}$. By a result contained in §2, $u \equiv (51)^{15} \pmod{59}$. This can be calculated more quickly by writing it as $u \equiv ((51^2)^2)^2(51^2)^2 51^2 51 \pmod{59}$ and hence we obtain that $u \equiv 46$ or $13 \pmod{59}$. Similarly the solutions of $v^2 \equiv 2588 \equiv 3 \pmod{47}$ are $v \equiv 35$ or $12 \pmod{47}$.

Now, the Euclidean algorithm yields that 4.59-5.47=1 and so the solutions of
$(2m + 1371)^2 \equiv 2588 \pmod{1773}$ are

$$2m + 1371 \equiv 5.47 \begin{Bmatrix} 46 \\ 13 \end{Bmatrix} + 4.59 \begin{Bmatrix} 35 \\ 12 \end{Bmatrix} \equiv \begin{cases} 341 \\ 1724 \\ 2432 \\ 2550 \end{cases} \pmod{2773}.$$

Hence $2m \equiv 1743, 353, 1061$ or $1179 \pmod{2773}$ and so $m \equiv 2258, 1563, 1917$ or $1976 \pmod{2773}$. The only value of m which corresponds to a pair of letters is 1917 which leads back to TR. The rest of the decryption is accomplished similarly.

References

[1] L. Adleman, K. Manders and G. Miller, *On taking roots in finite fields*, 20th IEEE FOCS **20** (1977), 175-178.

[2] L.M. Aldeman, C. Pomerance and R.S. Rumely, *On distinguishing prime numbers from composite*, Annals of Math. **117** (1983), 173-206.

[3] Gilles Brassard, *Modern Cryptology*, Springer-Verlag Lecture Notes in Computer Science **325**, 1988.

[4] Barry A. Cipra, *Math. team vault over prime record*, Science (25 Aug. 1989), p.815.

[5] H. Cohen and H.W. Lenstra, *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 297-330.

[6] A. Coyle, *Computer finds largest prime number*, The London Independent (31 Aug. 1989), p.3.

[7] W. Diffie and M.E. Hellman, *New directions in cryptography*, IEEE Trans. Info. Theory **22** (1976), 644-654.

[8] J.D. Dixon, *Asymptotically fast factorization of integers*, Math. of Computation **36** (1981), 255-260.

[9] J.D. Dixon, *Factorization and primality tests*, Amer. Math. Monthly (June 1984), 333-352.

[10] Patrick Fitzpatrick, *Asymmetric Cryptography*, IMS Bulletin **20** (1988), 21-31.

[11] M. Gardner, *Mathematical games, a new kind of cipher that would take millions of years to break*, Scientific American (Aug. 1977), 120-4.

[12] M. Garey and D.S. Johnson, *Computers and intractability; a guide to the theory of NP-completeness*, W.H. Freeman & Co., San Francisco, 1979.

[13] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford U.P., 1979.

[14] M.E. Hellman, *The mathematics of public key cryptography*, Scientific American (Aug. 1977), 130-9.

[15] Evangelos Kranakis, *Primality and Cryptography*, Wiley-Teubner, 1987.

[16] M.O. Rabin, *Digitalized signature and public key functions as intractable as factorization*, MIT Lab. for Comp. Sci. Technical Report **LCS/TR-22**, Cambridge, Mass. 1979.

[17] M.O. Rabin, *Probabilistic algorithms for testing primality*, J.Numb. Thy. **12** (1980), 128-138.

[18] Hans Riesel, *Modern factorization methods*, BIT **25** (1985), 205-222.

[19] Hans Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, 1985.

[20] R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), 120-126.

[21] H.E. Rose, *A course in number theory*, Oxford U.P., 1988.

[22] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, 1988.

[23] J. Seberry and J. Pieprzyk, *Cryptography: an introduction to computer security*, Prentice Hall, 1989.

[24] G.J. Simmons, *Cryptology: The Mathematics of secure communications*, Math. Intelligencer **1** (1979), 233-246.

[25] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comp. **6** (1977), 84-85.

[26] H.C. Williams, *Factoring on a Computer*, Math. Intelligencer **6** (1984), 29-36.

[27] Dominic Welsh, *Codes and Cryptography*, Oxford U.P., 1988.

Department of Pure Mathematics,
The Queen's University of Belfast.

An Elementary proof that periodicity and generalized-periodicity are equivalent in nilpotent groups

Gary J. Sherman

Let S be a non-empty subset of the group G. An element x of G is said to be S-periodic if there are elements $g_1, \ldots, g_n$ in S for which

$$\prod_{i=1}^{n} g_i^{-1} x g = e.$$

If $S = \{e\}$, then S-periodicity is the usual notion of group periodicity. If $S = G$, then S-periodicity is referred to as generalized-periodicity, a concept which occurs naturally in the theory of partially ordered groups. Indeed, a group admits a partial ordering relation compatible with the group operation if, and only if, the group contains an element which is not generalized-periodic [1]. Another case of special interest is when $S = P(G)$, the set of periodic elements of G. It was shown in [5] that $P(G)$ is a subgroup of G if, and only if, each $P(G)$-periodic element of G is periodic.

If G is abelian, then generalized-periodicity and $P(G)$-periodicity are equivalent to periodicity. Thus, when presented the class of nilpotent groups as a natural generalization of the class of abelian groups one asks: "Is generalized-periodicity equivalent to periodicity in the class of nilpotent groups?" Hollister [3] has shown that the answer to this question is yes. His proof makes use of a deep result from the theory of partially ordered groups and the fact that the periodic elements of a nilpotent group form a subgroup [4]. In this paper we give an elementary proof of Hollister's result and obtain, as a corollary, the fact that $P(G)$ is a subgroup for nilpotent G.

To this end the following two observations are useful. Let x and y be elements of the group G.

Fact 1. If x and y are periodic then xy is generalized-periodic.

Proof. Let x and y be of orders m and n, respectively. Then

$$\prod_{i=0}^{mn-1} x^{-i} x y x^i = x y^{mn} x^{mn-1} = e.$$