IAPetus

Quarterly Bulletin For the Institution of Analysts & Programmers

Issue 9 *April 1994*

Register of Consultants

Have we received your changes for 1994?

The Council has been considering how the Institution's Register of Consultants might be improved, so as to provide a better service both for members whose names appear in the Register, and for the many members of the public who telephone the Institution offices for help.

In 1995 it is likely that a radical step forward will be taken by splitting the Register away from the main Directory, so that it can be sold or otherwise made available to the public.

> *"a radical step forward will be taken by splitting the Register away from the main Directory"*

Skills categorised

At the same time a renewed attempt will be made to categorise members' skills, so that consultants suited to particular tasks can be identified electronically.

Our present system depends heavily on the DG remembering the entire membership, an increasingly difficult task for which he seems to have no special talent! Council Member Nick Swain reckons this is a poor show for a computing organisation, and has volunteered to do something about it.

The Register which appears in the 1994 Directory will be exactly the same as for 1993, unless you tell us you want something changed. A number of members have written already, and their changes have been logged. The deadline for any further changes is 16th May.

Register entries

There is no charge for an entry in the Register. If you would like one and have not had one before, all you need do is write or fax the essential information to the Institution Office.

If you wish you can give a business address and contact numbers for telephone and fax, in preference to the personal contact address which appears in the body of the Directory.

Up to 40 words are allowed for you to outline the services you have to offer. A quick look through last year's Register will provide some pointers on how to make the most of your entry.

Call for Papers

The 3rd IAP Conference is provisionally set for Friday 21st October at the City University, London (same place as last time).

Make space in your diary now, we'd be delighted to see you there. Even better, we'd like to hear you!

If you'd like to present a paper – or know someone who would make a good speaker – please call Nicole at the Institution office.

Inside this issue

The Director General writes...

Being a believer in doing the homework, before starting to write this I looked back at my last *IAPetus* message, written just before Christmas. At that time I anticipated 1994 with hope, but also with some apprehension.

The picture now, viewed from the relative comfort and security of the Institution office at least, is much brighter. We are beginning to hear news of members starting new contracts or getting promoted to better jobs. Instead of "I've lost my job and can't pay" we hear "I'm starting a new job and will send the money soon". Not quite like cash in the hand, maybe, but getting close.

The main thing that has cheered me personally is that at last our new Council is slipping into high gear. Policies are being put in place which will consolidate the Institution's position in the big league, qualitywise if not necessarily sizewise. (My spellchecker will hate those words!) We are beginning to reap the benefits of a broader intellectual input to the management of Institution affairs. Matters which were stalled because they required difficult decisions are now being tackled head on.

A decision has been taken to commission a new Coat of Arms from the College of Heralds. This should encourage members to publicise their connection with the Institution on personal and business stationary. It also means that at last we will have some ties and scarves that are worthy of the Institution and that members are proud to wear.

Following along the same line of thought, perhaps, we are investigating the pros and cons of seeking a Royal Charter. It has been made abundantly clear that while a substantial minority of IAP members are engineers, the majority do not want the IAP to go down the same route as the BCS to Chartered Engineer status. No, what we are interested in is true Chartered status for programmers – "C.Prog." or similar. ("C.Anal." somehow seems less suitable!)

It has also been agreed that the IAP ought to be seen at the major computing exhibitions. In the past we have been put off this by the cost and logistics of staffing such events. But the Council has decided that this is a high priority, and that it should be possible to pressgang local members to assist with manning the stands. So next time a letter from the Institution drops onto your mat, it could be a call to duty!

Michael C. Ryan
Director General

A Plea For Help...

Computing is a profession which often appeals to the "job changer", or the older person who decides to return to education.

Like all students, cash is a problem, and those of more mature years – particularly when used to actually earning money – really feel the pinch at times.

The other problem they face is that dreaded word "Experience". So, if any of you out there think that they could help by offering some vacation work, the Institution would like to hear from you.

Let us know what sort of tasks you need done, what skills you require – for example, if you supply software/consultancy etc. in retailing, someone who used to be involved in retail sales may well have useful experience, even while they are learning to program – and how much you can afford to pay.

Anyone who would like such a chance should also get in touch, students especially but anyone who feels the need for short-term experience – gaining employment as they change their career path.

We'll try and match you up.

Dear Sir,

Just to add to your collection of "urban myths".

I used to work in the advanced materials department of a university that shall remain nameless. Computers played an important role in research from data logging and analysis to simply writing letters.

You would think that with so much academic brain power someone would know how to work the PCs. Not at all. In fact there were only hand full of people who knew how to format disks.

Just before I left two lock-in amplifiers were bought. They cost £8,000 each and were the latest word in measurement technology.

Unfortunately, due to a badly written technical specification, they couldn't do the job they were supposed to and were consigned to the back of a cupboard. £16,000 down the drain? No, they had 3½" disk drives in them and could format a disk at the touch of a button. This is their sole function now!

I hope that brought a smile to your face!

Yours faithfully,

Paul Rattray

Programming in COBOL

Pre-owned Computeach course available at much reduced price.

Mr. Peter Bannister purchased a distance-learning course from Computeach, but due to an unexpected reorganisation at work he no longer has sufficient spare time to do it justice.

The course leads to a City and Guilds qualification in COBOL programming and normally requires part time study spread over a period of about two years.

Computeach have confirmed that they will accept the transfer of the course to a new owner.

The original cost of the course was £1,800, but it is now on offer to any member who is interested at a very substantial discount.

Telephone Peter Bannister on 0743 235051 (Work) or 0691 830 1650 (Home) or write to:
Penycoed,
Rectory Lane,
Pant, Oswestry
Shropshire SY10 8LG.

The time has come, the walrus said, to think of many things... This walrus is busy getting *IAPetus* organised before going on holiday! I shall think of you all slaving away over hot computers whilst chugging round the Indian Ocean!

More seriously, this issue of *IAPetus* heralds an important landmark in our Institution – the first real elections. Five places are available on the Council, to join the five appointed last year to get the thing going – and we have six candidates.

Each has been invited to "state their case", and their manifestos are elsewhere in this issue. So is the voting card, which is Reply Paid so you have no excuse not to vote... unless you actually don't want to.

The voting system to be used is a version of the Single Transferable Vote. Five places are up for grabs, and so you have five votes. You are to cast them in order of preference, i.e. number five people 1, 2, 3... as you choose.

You don't have to use all five votes if you don't want to. The candidate gaining the most "1" votes will be elected. All the "2" votes on the cards that had him as "1" will then be redistributed amongst the other candidates and the person whose total of "1" and "2" votes is the greatest out of the people left in contention will be elected. And so on.

Congratulations are in order for Seán Hickey, who was Technical Manager of a team which competed – very successfully – in the 1993 Computer Professionals of the Year Awards. Well done, Seán and friends... and do we have any more success stories out there? Let's hear them.

So, what else? Keep your articles, letters etc. coming... there's always space to be filled, and you don't want to have to put up with ME – and that's what will happen if there isn't enough material. You have been warned!

Enough from me, read the rest of *IAPetus*, hopefully enjoy.

Megan C. Robertson

Council Candidates

Leslie Almeida FIAP

I am a qualified IT professional with a BSc degree in Information Systems and a Post Graduate Diploma in Software Engineering.

My experience and expertise has been attained mostly in lecturing and consultancy work of which I have 14 years' experience working for Colleges of Further Education and in the IT industry.

I have taught Information Processing, Computer Science, Programming Languages, Structured Systems Analysis & Design and Application Packages. This involved developing course material, tutoring, project supervision & reporting and appraising student progress. I have liased with examination bodies (City & Guilds/Royal Society of Arts/London Chamber of Commerce & Industry/BTEC) and I'm a City & Guilds Visiting Assessor (Essex & Sussex Region) for the 726 Information Technology Scheme.

My main area of experience and interest lies in the IT Educational Sector.

If elected, I would like to design a Diploma Course specifically to fit industry requirements enabling students who would like a career in IT a better chance of job access. I would also like to create short courses in skill areas like Wordprocessing, Spreadsheets, Database Management Systems etc.

I would also like to work with other schools and colleges worldwide who would like to offer IAP certificates/diplomas and would like to validate their facilities and the courses they have designed should they differ from our syllabus due to market conditions in that particular country.

I hope this will result in an increase in the number of members worldwide. I will be grateful if I am elected into the council.

Gordon Bradley CmpnIAP

I was elected a Fellow of the Institution in October 1983 and, later, elevated to Companion in May 1989. I have been working in the area of computing for well over 30 years.

There are, at least, two aspects of the Institution that I feel should be more strongly addressed.

We are an international organisation and, as such, I feel that more members could and ought to be attracted from outside Britain. The membership is very much British based, even though many of them are registered as being overseas.

We should be encouraging more views, ideas and membership from other countries in the world. I am sure that we have much to give and much to gain from this.

With the ready availability of such things as Internet, CompuServe, etc., there would seem to be no reason why members from countries other than Britain could not be more closely involved.

As a very strictly "hands on" body we should strive to reduce the influence of others who are mostly run by "professional" committee members. Many of them are virtually in the hands of the manufacturers and some of the larger companies of, possibly, doubtful quality.

We should try to be far more of a prime mover in all areas of computing and computer education.

David Daniel FIAP

I have been working in the computer industry for over fifteen years, which seems like a lifetime considering the vast number of changes in our industry over that period.

Over the years I have lived and worked all over the UK and also abroad in Hong Kong and Malaysia. I can therefore hopefully understand the problems of foreign and ex-pat. IAP members better than most.

My main area of expertise is in the area of low-level programming, mostly on micro-processor based platforms including the omnipresent PC. I currently work in London on communications equipment for the world leader in financial information and news distribution.

I believe that the IAP has a very important role in our industry, especially in bringing together people

Continued on Page 4

Council Candidates – *Continued from Page 3*

from different areas and in promoting vocational skills.

Gavin Keeley, MIAP

I joined British Gas in 1985 on their graduate entry scheme and I gained my first commercial experience writing COBOL programs on ICL mainframes.

In 1987 I joined the consultancy firm Hoskyns and over the following two years undertook various assignments initially on mainframe systems, but then to a greater extent on PCs.

Having been the youngest person ever to be a Technical Consultant at Hoskyns, in 1989 I took the plunge and established myself as an independent consultant. Since then I have specialised in PC systems, especially in the area of Decision Support and Executive Information Systems.

My client base is primarily the top 10 UK companies and most recently my services have been provided to American companies. I have also been a guest speaker at conferences, and I now assist companies in building an IT strategy to utilise the new environments that have emerged in the last few years.

It is my belief that 1994 will see the start of the next revolution in our industry. The new operating systems and development tools that have been promised for so long, but which are now actually being delivered will, in my opinion, completely redefine the way in which our industry operates.

The traditionally segmented job roles of analyst and programmer will be lost forever into a much more hybrid role. The revolution will be fraught with many problems, but will also present opportunities to be more effective at delivering real benefit to our customers than ever before possible.

I hope to bring to the Institution my insight in this "brave new world" to assist other members in a smooth transition.

Ted Pugh AFA FIAP

Now 43 years old, I received an old Grammar-School education and served 3 years in Army Intelligence before joining the Rank Organisation as an auditor.

Nine years later I was recruited by Mecca Leisure to perform an in-depth systems and business analysis prior to its Stock Exchange flotation.

In 1985 I set up my own firm; began writing feature articles for the computer press in '89; designed and taught a C-based software engineering course for YTS/ET students and had a book published last year. My work stems mainly from Chartered Accountancy practices (via design and development of bespoke financial and business simulation software; assisting in computer audits; investigating fraud and consulting on related security matters).

I stand for: Continuing Professional Education (CPE); a Code of Ethics; member groups; an ombudsman; a recognised NVQ and establishing working parties on matters of major professional concern.

Our objective must be to achieve Chartered status.

Stewart Shuttle MIAP

Formerly with a Major International Bank, duties included: Correspondent Banker to banks in Scandinavia and the Netherlands; Credit Analyst; Business Development Officer – developing and designing marketing strategies and products for the International business markets; Project/Business analyst; reviewing and resolving a portfolio of foreign debt including the development of computer systems and audit procedures to satisfy the Inland Revenue.

Due to reorganisation, I was recruited by Hotel and Leisure Co as a Business Analyst/Consultant with a brief to exploit the benefits of computers to all members of personnel with the emphasis on developing marketing and financial awareness. This included developing training courses, brochures and organisational systems and procedures. Established BA Associates in May 1993 as a consequence of the above, as Business Advisor lately with emphasis on EDI.

Current assignments are primarily directed at smaller companies and include the following i) Marketing and Financial Analysis ii) Computer software utilisation iii) General Business analysis and methodology iv) and increasingly the development of Electronic Data Interchange (EDI).

The industrial segments covered included: Financial Institutions, Local government, Electroplating, Manufacturing and Distribution companies. Lately, invited participate in tendering for a consultancy contract in the former East Block for the establishment of the development of their Regional Development Agencies on behalf of the EEC.

Travelled internationally especially Scandinavia and Northern Europe, although thoroughly enjoy being at home in the garden or walking in Scotland or the Home Counties.

For your information: Static data – Age: 35, married, lived in Home Counties all the time. Member Luton Chamber of Commerce Institute of Directors, EDI Association. BA (Hons) in Business Studies.

Uses of Personal Computers in a Zoo

I had the good fortune to have been recently retired in 1986 and consequently, footloose and fancy free with minimal experience of PCs, spreadsheets and wordprocessing.

Being a member of the North of England Zoological Society, I trotted along to see the Director of Chester Zoo to discuss with him whether there was any way in which the Society could make use of my spare time. We discussed the mucking out of Elephants and the like but I expressed a preference for light duties and we eventually got round to the subject of spreadsheets instead of spreading muck.

When I arrived at the Zoo, the accounts department payroll, nominal, purchase and sales ledgers were maintained on a non-IBM computer system which in early 1987 was replaced by IBM AT/X kit using Omricon software. There was also one Amstrad PCW and one other wordprocessor used by the senior secretaries. Since then, the use of PCs in the Zoo has expanded enormously, as will be seen.

The NEZS is a scientific and educational charity of some stature, which receives no central or local government subsidy and consequently has to derive all its income from visitor admission fees, catering and shop sales. In order to look after the animals and some 450 acres of ground, 110 acres of which is open to the public, it employs a year round staff of some 160 persons (with the addition of temporary staff this rises to nearer 270 in the high season).

An operation of this order requires close budgeting and my first task was to create spreadsheet budgets for the 50 odd cost centres in the zoo instead of the pencil and paper budgets which had been prepared previously. My equipment was a Kaypro 64K CPM portable/luggable, shortly to be replaced by an Epson XT working at the speed of light (4.7 MHz). We must not knock the XTs. Over a period of years they have served us well and some are still in commission 7 years on.

The advent of the IBM compatibles saw us moving to Words and Figures for our non-accounting software requirements and for a number of years this package fulfilled all our wordprocessing and spreadsheet work needs and in fact, to this day, there are die-hards who still use WAF.

It soon became apparent that there were a number of peripheral financial and other statements which could more easily be produced as spreadsheets, analysis of cash books, statistics of visitor numbers, animal feeding requirements related to metabolic weight, tabulations of Superannuation Fund investments and the income therefrom, preparation of Animal Adoption Certificates, Coach Operators, Hotels, Tourist Information Centres and indeed for the Animals themselves.

ISIS (International Species Inventory System) had prepared an international database using compiled DBASE III, known as ARKS (Animal Record Keeping System) which became available to participating Zoos worldwide. This enables Zoos, not only to keep detailed records of their own stock, but also to access details of species or individual animals at other Zoos.

In the Zoological world, if inbreeding is to be avoided, it is most important to be able to find suitable mates for the animals (the staff are left to their own devices). Medical information and behavioural observations are all tools in the trade of animal husbandry. ARKS has often been compared with computer dating but is rather more wide-ranging than the latter.

Monthly updates of animal records are transmitted to ISIS in Minnesota, USA for inclusion in the world-wide database. In parallel with this, database software has been produced for use by the Studbook keepers of the various species and Medarks is available for the more detailed veterinary requirements of Zoological collections.

Chester Zoo shops market a very large range of gifts, souvenirs and toys, and a stock control program from Omricon was given a trial run. However, due to the multiplicity of items of stock, this was proving to be a sledgehammer to crack a nut and Quattro Pro spreadsheets were created to keep track of stock quantities and values. These have proved to be of particular value on the annual pilgrimage to the suppliers which is when the majority of the lines are re-ordered.

The Catering establishments have to date, declined to become involved with PCs on the grounds that they don't want to confuse bites with bytes! However, catering for the animals, which is the responsibility of the Animal Services Division, is a far more complex area. No "egg and chips twice" orders here!

Some 5,600 "animals" require feeding each day. Of these, 3,500 are fish and invertebrates but that still leaves over 2,000 mammals, birds etc. to be catered for. The animal diets run to hundreds of items, some produced by the ASD but most of which have to be bought in.

The twice weekly crack of dawn run to Liverpool Fruit and Vegetable market is a major shopping expedition (contrary to popular belief, our animals are not fed on rotting or second class produce – that would certainly be counter-productive in veterinary fees and could possibly result in the loss of specimens).

The annual shopping list includes some 87 tonnes of fruit (44 tonnes of apples, 30 tonnes of bananas and 13 tonnes of pears, grapes, oranges etc) and 121 tonnes of vegetables. The cost of all foodstuffs is charged out to the various Animal Cost Centres for budgetary purposes with the

Continued on Page 8

"my first task was to create spreadsheet budgets for the 50 odd cost centres"

"Monthly updates of animal records are transmitted to ISIS in Minnesota, USA for inclusion in the world-wide database"

A QUESTION

One issue facing both bespoke developers and system managers alike concerns adopting a suitable set of encryption algorithms as a last means of defence against unauthorised system access.

There are a number of ways to approach this problem – perhaps the best known being to apply IBM's Data Encryption Standard (DES). Unfortunately, although details of this algorithm have been placed in the US public domain (and are readily available world-wide) IBM still retains its rights in all other territories.

Making unauthorised use of this algorithm is therefore fraught with difficulties, and there have in any case been some doubts expressed regarding its absolute security.

"it is often as important to confirm the identity of a correspondent as it is to ensure material confidentiality"

DES doubts

Diffie and Hellman – participants in the workshop held by the US Federal Bureau of Standards to examine DES back in '76 – discovered a quasi-linear weakness in the selection functions and a complementary symmetry between plaintext and its encryption.

It is also fair to say that basic DES is not suited to encrypting large series of repeating characters or large volumes of data, since the analysis of such cipher-text can greatly simplify key extraction. Furthermore, should just part of a DES key be compromised, discovering the remaining elements can be relatively easy.

The Vernam cipher

A technique used by many "off-the-shelf" packages is therefore based on the Vernam cipher. Here, a key is used to generate a unique stream of pseudo-random numbers that are individually XORed with the plaintext to produce an encrypted version. This has the advantage over DES of being very fast in operation – but its weakness lies in the pseudo-random nature of the XOR stream. If the algorithm used to generate the random numbers is known, then a "brute force" attack can be launched by simply programming a computer to try each possibility.

When applying the Vernam technique, it is therefore crucial to ensure the chosen algorithm produces an extremely large stream of "random" numbers before it inevitably begins to repeat. This is particularly important when the algorithm's details are contained in an application that may be freely purchased by others.

The single-key weakness

Of course, the main problem with using techniques like those described above, lies in having to physically secure the encryption key. This is not easy when a number of authorised users are involved.

Once a key has been compromised, a third party may easily decrypt confidential data and (should they wish) encrypt data as well. The latter is a vital point, often overlooked by many users, system managers and analysts. Especially in the area of secure communication traffic over the public network, it is often as important to confirm the identity of a correspondent as it is to ensure material confidentiality.

Unfortunately, single-key systems do not lend themselves easily to this task.

An unbreakable cipher

Outside the murky portals of the Intelligence and Security Services, only one cipher can be said to be, to all intents and purposes, unbreakable. This is the RSA cipher developed in 1977 at the MIT by Ronald Rivest, Adi Shamir and Leonard Adleman.

Until recently, the main argument put forward against its deployment was that of speed; but with the universal availability of high-speed processors now available, this objection is no longer valid.

RSA overview

The RSA cipher is mathematically based, with its putative security resting upon the "impossible" task of producing a prime number generator. Like the ubiquitous travelling salesman problem, this appears to have no solution in polynomial time and is classified as a non-deterministic polynomial complete (or NP) problem.

The RSA uses large prime numbers (of around 100 to 200 digits in length) and its solving is equivalent to trying to factor an extremely large prime. Numerous attempts have been made to crack it since its inception; but all have so far failed.

RSA algorithm

The RSA cipher is implemented as follows:–

1. Take two large prime numbers, P and Q, and multiply them together to give M.
2. Compute the members, R, of the reduced residue set for the modulus M. Since both P and Q are both prime this will be equal to (P–1)(Q–1).
3. Select an encryption key, E, of this set; such that E is greater than two and the greatest common denominator between E and M is one.
4. Now find E's inverse, D; such that ED = k0[M]+1 = 1 mod 0[M]. That is, the product ED, less one, results in a remainder of zero when divided by R.
5. Retain E, D and M; but destroy the other data for security reasons.

Public-key ciphers

RSA was intended for use as a public-key cipher. Unknown correspondents could be invited to send secure transmissions by publishing either E or D, in conjunction with M and an agreed block size. If E were published, D would be kept secret by the code's designer. In the same

"only one cipher can be said to be, to all intents and purposes, unbreakable"

OF SECURITY

way, should D be published, E would have to be secured.

To encrypt a message, its plain-text is broken down into the required byte block-size and thus treated as a single, large binary number. This is raised to the published power and then reduced modulo M. The process is repeated for each character block.

Decryption can only be performed by the code's instigator and is achieved by raising each number to the power of the unpublished key – and again reducing the result modulo M. This results in the cipher's conversion to its original plain-text form.

The method is both simple and extremely secure – provided the primes P and Q are chosen with care. The problem then presented to an hostile cryptanalyst is equivalent to the task of factoring M (a task, given two large primes, that would take millions of trillions of years).

Large prime generation

Generating a P and Q of the required size is not so difficult as might first be supposed. A computer is simply programmed to generate a number of the size needed and this then tested for probable primality – either by dividing it by a series of pseudo-random numbers of applying a test based on Fermat's (little) theorem.

Tests associated with quadratic and non-quadratic residues may also be employed if desired. The resulting "probable prime" can then be tested on some suitable plain-text to ensure no problems arise.

Signature blocks

With a public-key cipher, only the intended recipient can decipher the encrypted message. Moreover, if a code's designer chose to encrypt a message using his private half of the key, any correspondent could read it. But – and here is the important point – only the code's originator could have encrypted it in the first place.

Obviously we wouldn't wish correspondents to determine our private key by analysing a signed message; but we can overcome this obstacle by simply publishing details of a further code that can be used to decrypt our signature block – and correspondents can do the same.

When a message is encoded, communicants encrypt a signature using their private half of the appropriate key, then append this to the required plain-text message and encrypt it (along with the appended signature) using the intended recipient's public details. (The signature block thus receives double encryption.)

The result is a message with a verifiable source, suitable for putatively secure transmissions over the public network.

No other method comes close.

Public key flexibility

Ciphers that use separate keys for encryption and decryption can be particularly useful in the realm of permitting system access.

Most members will know how easy it is to gain unauthorised access to simple password-protected installations; but utilising a public key cipher can overcome this problem.

The secret lies in having authorised personnel register a public key with the main system and then use their private half to encrypt and send the current time and date once primary log-on has been established. Before granting full access, the system decrypts the encoded message and confirms that the resulting plain-text is correct. Only then is the user granted appropriate access.

Naturally, any confidential data transfer also requires adequate protection, but the system outlined overcomes the problem of a possible "eaves-dropper" logging back on once the line is clear.

I believe this method has far more to commend itself than standard "call-back" or exotic "key-press rhythm" techniques – both of which can be circumvented in practice.

Other RSA users

For those readers frustrated with the few registrations obtained from launching a shareware product; RSA can provide a convenient solution.

Many enterprising authors have, in the past, attempted to impose some form of time constraint on a freely-distributed program – but have been thwarted by the ingenuity of users to circumvent it. The problem, of course, lies in having the stop-date – or the decryption algorithm used to recover it from an external file – contained in the application's code.

"Numerous attempts have been made to crack it since its inception; but all have so far failed"

With a single-key cipher, a pirate can recover the algorithm via disassembly and reverse-engineer a new date to be used. But by using the RSA method, the program can only decode enciphered data. The way it has been encrypted remains the author's secret alone.

It takes just a small stretch of the imagination to see how this technique can be used to permit commercial hiring of software.

Naturally, using RSA by itself does not stop pirates inserting code that jumps around the program's security – nor does it prevent them from removing the security code completely; but there are a number of techniques available to mitigate this type of problem.

Implementation obstacles

The only drawback to implementing RSA is that no programming language supports integers of sufficient length.

In order to make proper use of the technique, suitable mathematic routines must first be developed. While this is in fact possible using any modern language with in-line assembler support, undertaking the task in direct assembler has two considerable advantages: code size is dramatically reduced and execution speed significantly enhanced.

Continued on Page 8

A Question of Security – *Continued from Page 7*

On offer

For those IAP members who wish to implement RSA, or who have other reasons for supporting extremely large integers (but don't have the time – or patience – required to undertake the necessary assembly coding themselves) I am making available the basic maths functions that I have developed for the PC.

For obvious reasons I am not placing this code on general sale; and I am also asking all interested members to ensure that it is properly protected from falling into criminal hands. (Members may freely use it to develop their own commercial applications – for which they can charge criminal prices – but let's not make the Police's task more difficult than it already is).

On offer are assembler sourced routines to implement the manipulation of very long numbers. These include support for: addition; subtraction; multiplication; raising to a power; extracting the square and nth roots; computing gcds and calculating a key's inverse – plus outputting these numbers in base 10 format. In fact, all you need to include RSA in your own applications, provide support for large numbers in general – or provide a basis for developing additional functions.

The code is available in three forms: library; object and MASM source – with the latter constructed to permit simple reconfiguration and minimum stack usage.

Library and object code versions permit numeric calculations of up to 2,555 digits in length (which should be more than adequate in practice) while the source code only requires a small EQUate changing to permit far larger numbers to be handled.

Full support is provided for all four Intel memory models – but members need to specify which calling convention is required when ordering either libraries or object code (C or Pascal/FORTRAN/BASIC).

Purchasers of the source code can simply modify the language and model defines at compile time to generate their own particular requirements.

Libraries and object code versions are each available for just £10; the MASM source code for £25.

Please note this offer applies only to IAP members – the last time I offered my C User Interface Library I was also deluged by non-member requests. Also, as an aside to those members who have purchased my book: thank you for your support, but please note you don't have to go through my publisher to obtain the professional version. Just £10 to myself will suffice – and your programs will then be able to do everything Windows can in just 128K RAM on an old text-based 8088 – but fast (The non-member price is £30 with proof of book purchase or £80 without).

If any member reading this has erroneously taken the publisher route: please let me know so I can refund the difference.

UK residents should add VAT to the prices quoted above and members living abroad should enclose suitable international reply-paid coupons. Cheques only drawn on a UK bank or international money-orders please – and don't forget to indicate the disk size you require.

My address is contained in the consultant's section of the IAP's Directory of Members.

Ted Pugh AFA FIAP

Personal Computers in a Zoo – *Continued from Page 5*

help of Quattro Pro spreadsheets which are also used to control stocks of feed.

The Marketing Department have many facets to their work quite apart from the shops and catering establishments. The Membership Secretary maintains records of some 8,000 Members and Animal Adopters. The Party Office has a similar number of records on their database and, together with other members of the administrative staff, use DTP (currently PagePlus) for the production of menus, certificates, leaflets, signs and even the draft of the Zoo Magazine before it is sent to the Printer. Many artistic and creative hours have been spent in this way.

The Estates Division have responsibility for all Gardens (a major attraction of this Zoo and one which has captured many awards), car parks and grounds, buildings, vehicles and machinery, and the maintenance thereof.

Spreadsheets are used to monitor the consumption of fuel (gas, electricity and oil), to control the flow of maintenance requests, to establish a planned maintenance routine for all machinery (including pumps and boilers) and to prepare a list of priorities for future projects. They have recently purchased CAD software for the preparation of plans and drawings.

Personal computers have played an important and ever increasing role in the day to day running of the Zoo.

Some LANs (Local Area Networks) are already in operation and others are planned. Omricon, PagePlus, Visionsoft, Paradox and Quattro Pro are the software packages on which we have standardised but we are still using Words and Figures, Lotus Works, Symphony and Cambase to some extent.

The use of PCs in the Zoo will doubtless be extended in the future as it has done in the past.

Derrick C. Thompson

IAPetus is the Quarterly Bulletin of the **Institution of Analysts and Programmers.** The Editor is Megan C. Robertson. All views expressed herein are those of the authors, and do not necessarily reflect the Institution's or *IAPetus*' opinions or position. Produced by Breeze Ltd, 061-792 4442.
Correspondence about *IAPetus*, contributions etc. should be sent to the Editor at 12 Bude Close, Crewe, Cheshire CW1 3XG (Tel: 0270 500565). Correspondence about the Institution should be sent to Charles House, 36 Culmington Road, London W13 9NH (Tel: 081 567 2118, Fax: 081 567 4379).