Factorizar . . . é fácil?

Numa revista em que os Números e a Álgebra são os principais temas, talvez fosse interessante tentar enquadrar de algum modo esta secção no tema da revista. Resolvi interromper o texto em que estava a trabalhar e tentar responder a esta sugestão da Redacção. Como o tempo era muito limitado conversei com um colega nosso**, para quem a teoria de números é uma das principais áreas de interesse, que muito amavelmente, me sugeriu e me deu indicações sobre o tema dos números primos e da factorização de números inteiros e consequentemente a criptografia, assunto que só abordarei muito ligeiramente, limitando-me a indicar apenas alguns sites onde o assunto é tratado.

Factorização e números primos porquê? Porque são assuntos muito comuns nas aulas.

A factorização é um tema que os nossos alunos tratam desde muito cedo, de um modo necessariamente muito básico, mas que a outro nível apresenta uma enorme complexidade.

Com toda a tecnologia disponível hoje em dia, saber se um dado número inteiro é primo ou não, é uma questão *relativamente* fácil de responder. Se o número não é primo então pode decompor-se num produto de pelo menos dois números primos. Este problema, já não é tão *fácil* e é mesmo um problema em aberto o de encontrar qual o melhor algoritmo para fazer uma factorização. Claro que isto se passa quando nos estamos a referir a grandes números.

Para ter uma ideia do grau de dificuldade basta navegar um pouco pela página da RSA Laboratories. Esta empresa, especialista em codificação de dados tem na sua página um desafio em que propõe a factorização de oito números a que chama números RSA. Atribui prémios muito interessantes, que vão dos 10.000 dólares e podem chegar a 200.000 dólares, que dizem ser apenas prémios simbólicos, tendo em conta todo o trabalho envolvido na sua resolução.

Esses números-RSA são do tipo utilizado pela empresa nos seus códigos e cada um deles é o produto de apenas dois números primos.

No site diz-se que, com a tecnologia existente e os algoritmos que se conhecem, factorizar números com 100 algarismos, é bastante fácil. O mesmo já não acontece para números com 200 algarismos. O desafio que a empresa propõe serve apenas para a própria empresa verificar quais os avanços que estão a ser feitos nesta *arte* da factorização, para estar um passo à frente de possíveis quebras das suas chaves de codificação.

O último número-RSA que foi factorizado (Dezembro de 2003) tem 174 dígitos. A empresa prevê que o oitavo número-RSA proposto, constituído por 617 algarismos, demore ainda décadas a ser factorizado.

Quando um número é factorizado isso não significa que se percam as chaves de segurança e que estas tenham logo de ser substituídas por outras maiores. Tudo depende do tempo gasto, do número de computadores envolvidos nesse trabalho e da finalidade do código.

Porquê um número que é um produto de apenas dois números primos?

Para quem já leu alguma coisa sobre criptografia não é estranho este facto nem esta sigla RSA.

RSA é um algoritmo criado em 1978 por Ron Rivest, Adi Shamir e Leonard Adleman destinado à criptografar dados. É muito utilizado em protocolos de comércio electrónico e é bastante seguro, com chaves relativamente longas.

O algoritmo não é muito complicado de entender. Baseia-se essencialmente num par de números que constituem a chave pública e num terceiro número que é a chave privada. Escolhem-se dois números primos muito grandes (P e Q) e começa-se por calcular o produto PQ. Segue-se a escolha de um inteiro ímpar E, menor que PQ e primo com $(P-1)(Q-1)$.

O par $(PQ,\ E)$ constitui a chave pública.

A chave privada é um número D, tal que $(DE-1)$ é divisível por $(P-1)(Q-1)$.

A função de codificação é $C = (T\hat{}E) \bmod PQ$, sendo C o resultado da codificação e T o número a codificar. T terá que ser inferior a PQ.

A descodificação é feita por $T = (C\hat{}D) \bmod PQ$.

Não se conhecem métodos simples para calcular D, P e Q partindo apenas do par $(PQ,\ E)$, por esse motivo a chave é pública, não há qualquer problema em ser conhecida. O *segredo* está no valor de D que não poderá ser revelado.

Se visitar a página `http://world.std.com/~franl/crypto/rsa-guts.html` encontra uma explicação simples dos passos a seguir para fazer uma codificação e a respectiva descodificação, seguindo este algoritmo, assim como um exemplo prático onde tudo se torna mais claro.

Pode encontrar também a explicação do algoritmo RSA consultando a Wikipedia em:

`http://en.wikipedia.org/wiki/RSA`

Para ganhar *alguns* dólares basta consultar o site `http://www.rsasecurity.com/rsalabs/node.asp?id=2093` e tentar factorizar um dos números-RSA. Porque não o mais simples? o RSA-640?

```
3107418240490043721350750035888567930037346022
8427275457201619488232064405180815045563468296717232867824379162728380334154710731085019195485290073377248227835257423864540146917366024776523466609
```

Tem apenas 193 dígitos!

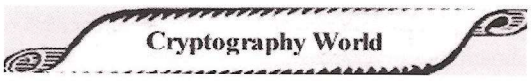
No site desta empresa encontrei alguns dados que achei interessantes, pelo menos para uma pessoa que não tem conhecimentos nesta área, como é o meu caso.

Por exemplo, na secção dos boletins, o boletim número 13, tem entre muitas outras coisas, uma tabela dos records de factorização desde 1970 até 1999 e o gráfico que relaciona o número de dígitos do número factorizado num determinado ano com o respectivo ano. Chamam a atenção para uma certa linearidade deste gráfico e para as razões possíveis para isso acontecer, uma vez que dado os grandes avanços tecnológicos seria de prever uma relação exponencial.

** António José Machiavelo, professor no Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto

Navegando na Internet

Os sites sobre criptografia são imensos, uns bastante complicados para quem quer fazer uma primeira abordagem ao assunto, mas alguns têm, indicações bem mais simples como por exemplo o site:



`http://www.cryptographyworld.com/index.htm`

destinado essencialmente a quem quer iniciar o estudo deste tema, tratando conceitos básicos, chaves e os diferentes algoritmos.

No site da World Wide Web Virtual Library em:

`http://world.std.com/~franl/crypto.html`

encontra ligações para muitos sites sobre a criptografia, incluindo artigos, organizações, perguntas frequentes, etc, além da descrição do algoritmo RSA, já indicado no texto.

No site da Revista da Armada

`http://www.marinha.pt/extra/revista/ra_jan2004/pag_10.html`

encontra-se um artigo onde é feita uma síntese histórica da criptografia, desde o antigo Egipto até aos nossos dias.

E chega de cálculos complicados, que exigem supercomputadores ou um grande número de computadores a trabalhar em simultâneo. Vamos fazer cálculos mais simples. Que tal utilizar uma máquina de calcular que efectua cálculos em numeração romana?

Está em:

math.com℠
The World of Math Online

`http://www.math.com/students/calculators_pre_ti/roman/compvterromanvs.html`