Noite Europeia dos Investigadores

Alice, Bob e o Computador

Imagine que pretende enviar uma mensagem com conteúdo secreto a Bob. Imagine que acordaram num tipo de cifra semelhante à Cifra de César. Pode ser mais ambicioso e escolher uma outra da mesma família, bem mais complexa e mais protegida aos ataques de um intruso. Há, no entanto, um passo que pode ser identificado como crítico: a troca de chaves. Por exemplo, na Cifra Shift terá que combinar com Bob qual o deslocamento do alfabeto que fez.

Refira-se que, apesar deste problema inicial, as cifras que exigem uma troca de chaves iniciais podem ser seguras. Aliás, são usadas extensivamente nas comunicações seguras actuais (como o AES).

Uma resposta a este problema de troca de chaves surgiu em 1977, por Rivest, Shamir e Adleman. Propuseram a cifra de chave pública **RSA**. De uma forma sucinta, Bob publica para o mundo o que denomina por chave pública. Esta é constituída por um produto de dois primos distintos e pelo denominado expoente de cifração que satisfaz algumas condições técnicas. Bob mantem secreto os números primos que usou. Para enviar uma mensagem a Bob, basta usar a chave pública que este revelou ao mundo.

BOB cria a chave:
escolhe **p**, **q** números primos: **p**=53, **q**=67;
determina **n**=**pq**=3551
e **m**=(**p**-1)(**q**-1)=3432;
escolhe **e** tal que m.d.c(**e**,**m**)=1: **e**=7;
determina **d** tal que o resto da divisão de **ed** por **m** é 1: **d**=1471;
chave pública: (**n**,**e**)
chave privada: **d**

ALICE pretende enviar código de multibanco a BOB: **mens** =1234.
Cifra a mensagem usando a chave pública de BOB (**n**,**e**): determina o resto da divisão de **mens**^{e} por **n**; obtem **cifr** = 3063.
Envia **cifr** a BOB.

BOB recebe a mensagem cifrada e decifra-a usando a sua chave privada **d**: determina o resto da divisão de **cifr**^{d} por **n**; obtem **mens** = 1234.

Em que se suporta a segurança do RSA? Acredita-se que quebrar o RSA é equivalente a factorizar em números primos o número que Bob publicou, e que este é um problema difícil, ou seja, nenhum computador resolve este problema de forma eficiente. O caso muda de figura se alargarmos o conceito de computador, de modo a incluir o computador quântico.

Porque não se usa apenas o RSA nas comunicações seguras? Comparando com os sistemas "simétricos" (como o AES), é pouco eficiente... sendo 100 a 1000 vezes mais lento que o DES, por exemplo. Na prática, usa-se um sistema "híbrido": o RSA (ou outro semelhante) para a troca de chaves, e um "simétrico" (como o AES) para efectivamente se trocar informação.

Onde está o RSA na sua vida? Abra um browser e uma página que use o protocolo https (facebook ou e-mail, por exemplo); veja as definições de segurança dessa página e encontrará a chave pública RSA usada...

Universidade do Minho
Escola de Ciências
Departamento de Matemática e Aplicações