Como Alice e Beto podem se comunicar sigilosamente pela Internet

Uma carta pelo sistema de chave pública: um exemplo de criptrografia

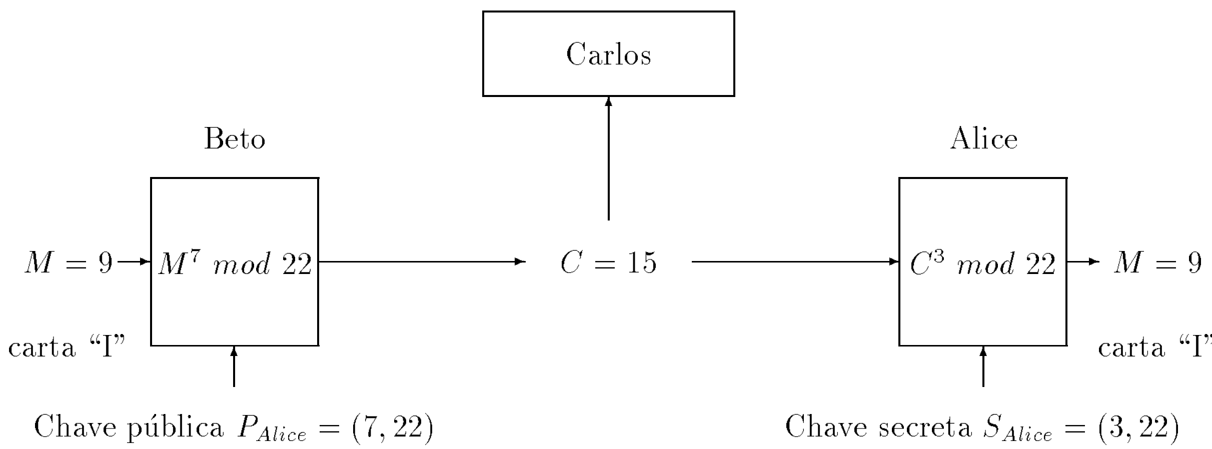
Routo Terada - Depto. de Ciência da Computação da USP, 1997

Vamos supor que Beto quer enviar uma carta de amor muito sigilosa, que chamaremos M, para Alice. Os dois estão geograficamente distantes e cada um possui um microcomputador à sua disposição para se comunicarem, via modem e linha telefônica, pela Internet. Obviamente, Beto não deseja que algum intruso Carlos que possa "grampear" M na linha consiga entender a carta M.

No dia anterior, prevendo a intenção do Beto, Alice havia tomado o cuidado de calcular no seu micro duas chaves:

1. a sua chave secreta S_{Alice} que vale, por exemplo, $(3, 22)$ (i.e., par de inteiros 3 e 22),
2. e também a sua chave pública P_{Alice} que vale, por exemplo, $(7, 22)$ (i.e., outro par de inteiros relacionado matematicamente com o par $(3, 22)$, como veremos mais tarde). Nas situações reais estas chaves são mais longas, da ordem de dezenas de algarismos.
3. Ademais, Alice havia enviado a chave $P_{Alice} = (7, 22)$ para Beto.

Para ilustrarmos, vamos supor que a carta se resume à letra "I", a nona letra do alfabeto. Por isso, Beto faz corresponder à letra "I" o número 9.



1. Beto conhecendo a chave pública $P_{Alice} = (7, 22)$ calcula no seu micro o valor $9^7 \ mod \ 22 = 15$ (i.e., resto da divisão por 22 do resultado de 9 elevado à potência 7) e envia 15 para Alice.
2. Ao receber 15, Alice conhecendo a chave secreta $S_{Alice} = (3, 22)$, calcula o valor $15^3 \ mod \ 22 = 9$, isto é, ela recupera o valor original correspondente à letra "I".

Se eventualmente Carlos, o intruso, conseguir "grampear" o número 15 da linha, ele não consegue recuperar o valor 9, pois ele não conhece a chave secreta da Alice $S_{Alice} = (3, 22)$. Em outras palavras, o valor 15 é ininteligível para Carlos.

Genericamente os cálculos efetuados das duas chaves pela Alice são os seguintes (estes passos são uma variação do sistema conhecido por RSA, iniciais dos autores R. Rivest, A. Shamir e L. Adleman que, na época, eram pesquisadores no MIT, EUA.):

Cálculo de um par de chaves

1. Calcular dois números inteiros primos e longos (i.e., com dezenas de algarismos) chamados q e r; e calcular o seu produto $n = q.r$. (No exemplo acima, $q = 2$ e $r = 11$.)

2. Calcular um terceiro número primo chamado s e calcular um inteiro p que satisfaça $p.s = 1 \; mod \; (q-1)(r-1)$ (No exemplo acima, $n = 22$, $s = 3$, e $p = 7$.), através de uma variação do Algoritmo de Euclides para calcular o Máximo Divisor Comum – MDC que aprendemos na escola secundária (aquele em que usamos a propriedade de $MDC(f, g) = MDC(g \; mod \; f, f)$, onde $f < g$ são inteiros positivos, como em $MDC(12, 42) = MDC(6, 12) = 6$).

3. A seguir Alice apaga os números q e r no seu micro.

4. A chave secreta $S_{Alice} = (s, n)$ é guardada com cuidado pela Alice e a chave pública $P_{Alice} = (p, n)$ é enviada para qualquer pessoa amiga da Alice (pode até ser incluida em uma lista de chaves públicas semelhante a uma lista telefônica, contendo as chaves públicas de todos os usuários da rede de computadores Internet).

Nestas condições, considerando uma carta expressa como um número inteiro M entre 0 e n, são efetuados os passos seguintes (Por exemplo $M = 941$ para a carta "IDA".):

Envio de carta

1. Beto calcula e envia para Alice $M^p \; mod \; n = C$, onde p e n são da chave pública da Alice. (C é chamado código criptografado de M.)

2. Alice recebe C e calcula $C^s \; mod \; n$ que deve ser igual a M. (Pode-se provar que de fato $C^s \; mod \; n = M$, utilizando um teorema antigo chamado Teorema de Euler.)

Autenticação do Destinatário

Veremos a seguir que Beto tem certeza que só a Alice autêntica pode recuperar M. Esta certeza chama-se *Autenticação do Destinatário*. Note que Alice não tem certeza que Beto enviou C para ela, pois a chave (s, n) pode ser utilizada por qualquer pessoa.

Mesmo quando Carlos consegue o valor C, ele não consegue recuperar rapidamente o valor M da carta original (i.e., "quebrar" o código C) pois só a Alice conhece a chave secreta $S_{Alice} = (s, n)$. Além disso, Carlos ou qualquer outro intruso *não* consegue recalcular rapidamente o valor s na chave secreta (s, n) (i.e., "quebrar" a chave) da Alice *mesmo* conhecendo C e a chave pública (p, n) da Alice.

Calcanhar de Aquiles

Tomamos o cuidado de dizer "rapidamente" nas duas sentenças anteriores pois este sistema possui um "calcanhar de Aquiles": se Carlos conseguisse fatorar o número n em primos q e r, então ele poderia calcular s que satisfaça $p.s = 1 \ mod \ (q-1)(r-1)$ como efetuado por Alice no passo (2) do cálculo de um par de chaves. O ponto importante aqui é que até hoje não se conhece um procedimento *rápido* para fatorar um número n "longo" em primos, e consequentemente Carlos não consegue recalcular a chave secreta da Alice rapidamente explorando esse "calcanhar de Aquiles", mesmo que ele seja um estudioso do assunto, e tenha um super-computador à sua disposição. Para ilustrar, quando o número n possui cerca de 100 algarismos decimais, Carlos teria que gastar cerca de 70 anos de um super-computador da última geração, utilizando o procedimento mais rápido que se conhece, de autoria de um matemático chamado R. Schroeppel; e cerca de dez milhões de *séculos* se n possui cerca de 200 algarismos!

É importante mencionar que até hoje os pesquisadores não conseguiram descobrir qualquer outro ponto fraco neste sistema de criptografia.

Autenticação do Remetente

Vamos supor agora que além do par de chaves $S_{Alice} = (s, n)$ e $P_{Alice} = (p, n)$, existe um outro par $P_{Beto} = (p', n')$ e $S_{Beto} = (s', n')$ calculados por Beto, com $n' < n$. O envio de carta é alterado para:

Envio de carta com outro par de chaves

1. Beto calcula $M^{s'} \ mod \ n' = A$, onde s' e n' são da chave secreta do Beto (A é chamado código de M assinado por Beto).
2. Beto calcula $A^p \ mod \ n = C$, onde p e n são da chave pública da Alice.
3. Beto envia C para Alice.
4. Alice recebe C e calcula $C^s \ mod \ n$ onde s e n são da chave secreta da Alice. Esse valor deve ser igual a A, pois (s, n) é a chave que desfaz o que a chave (p, n) faz.
5. Alice calcula $A^{p'} \ mod \ n'$ que deve ser igual a M, pois (p', n') é a chave que desfaz o que a chave (s', n') faz.

Neste novo procedimento de envio de carta para Alice nós temos as seguintes propriedades muito importantes em redes de computadores como a Internet:

1. *Autenticação do Destinatário* (que já existia no procedimento anterior) pois só a Alice autêntica possui o valor s utilizado para converter C em A e assim Beto tem certeza que só a Alice verdadeira pode ter recuperado M.

2. *Autenticação do Remetente*, isto é, Alice tem certeza que só o Beto verdadeiro pode ter enviado C para ela, pois só Beto conhece o valor s' utilizado para converter M em A (portanto A merecidamente recebe o nome de código de M *assinado* por Beto).

"Cheque" eletrônico

Além destas duas propriedades importantes, temos outra: Alice não consegue alterar M para um outro valor M' e dizer ao Beto que recebeu este valor no lugar de M, pois Beto vai exigir, em caso de disputa, que Alice exiba o valor A' correspondente a M', e Alice não conseguiria calcular A' a partir de M' sem conhecer s' da chave secreta do Beto. Esta última propriedade é essencial em redes de transferência eletrônica de fundos, em que M corresponde, por exemplo, a um "cheque" de um certo valor M para Alice "sacar" e ela não consegue alterá-lo para um valor M' maior que M.

Routo Terada (Internet: rt@ime.usp.br) é Professor Titular no Depto. de Ciência da Computação da Universidade de São Paulo, e possui grau de Ph.D. em Ciência da Computação pela Universidade de Wisconsin-Madison. Suas áreas de pesquisa incluem Criptografia, Complexidade de Computação, e Aprendizagem por Computador