

CRIPTOGRAFIA ASSIMÉTRICA PARA SEGURANÇA DE SISTEMAS DISTRIBUÍDOS

Pedro Venda
Instituto Superior Técnico, Universidade Técnica de Lisboa
Portugal
pjlv@mega.ist.utl.pt

Resumo

A segurança de sistemas distribuídos é uma necessidade e a utilização de técnicas que envolvem a criptografia assimétrica garantem uma solução elegante para a confidencialidade e assinatura digital de mensagens. Muitas aplicações conhecidas utilizam criptografia assimétrica directa ou indirectamente. A sua simplicidade e forte segurança possibilitaram a adesão por parte das empresas e da comunidade.

Palavras Chave

sistemas distribuídos, criptografia assimétrica, chave pública, chave privada, criptografia, assinatura digital, certificado, CA

Introdução

A necessidade de segurança em ambientes distribuídos surge naturalmente quando estes processam informação sensível. Num sistema distribuído, processos ou utilizadores são **entidades** que pretendem comunicar e, no âmbito considerado, serão tratados da mesma forma.

Em geral, um sistema distribuído consiste numa rede de meio partilhado, em que todos os nós ligados a esse meio conseguem “ver” todas as mensagens trocadas entre quaisquer outros nós dessa rede. Desta forma, uma entidade “mal intencionada” pode ver e interpretar o conteúdo da comunicação entre duas entidades alheias, residentes em diferentes nós da rede. Tal comunicação não é segura, pois o nó “mal intencionado” pode registar, alterar, adicionar, retirar, repetir ou trocar a ordem das mensagens trocadas, dependendo da topologia, posicionamento na rede e tecnologia utilizada.

A segurança num sistema distribuído passa pela autenticação de entidades e respectivo controlo de acesso aos recursos e pela criação de canais seguros de comunicação entre entidades em nós possivelmente diferentes. Tais canais terão que garantir confidencialidade, integridade e autorização [1]. **Confidencialidade** refere-se à propriedade da informação. O emissor de uma determinada mensagem

detém direitos sobre ela no sentido em que decide quem pode entendê-la. A **integridade** garante que a mensagem chega ao receptor inalterada. Alterações não autorizadas serão facilmente detectáveis. A **autorização** é utilizada para aferir se cada entidade está devidamente credenciada para aceder aos recursos que pretende [1].

A possibilidade real da ocorrência de ataques ao sistema distribuído requer a definição de conceitos adicionais. Os tipos de ataque possíveis [2] originados por uma entidade são a visualização, a interceptação (e/ou retenção), a alteração e a introdução de mensagens.

A encriptação (utilização de técnicas de criptografia), a autenticação, a autorização e a auditoria de entidades ou sistemas utilizam-se para prever, combater e/ou analisar tentativas de ataque (ou mesmo ataques bem sucedidos).

A definição de um sistema seguro é subjectiva, dado que um sistema pode ser seguro para determinada tarefa mas vulnerável para outra diferente. A política de segurança de um sistema define a exigência do mesmo face às possíveis vulnerabilidades.

A criptografia é um mecanismo essencial à quase totalidade de sistemas de segurança, pois permite garantir não só confidencialidade, como também integridade, autenticação e autorização.

Criptografia

A criptografia é uma técnica de processamento de dados que procura “disfarçar” as mensagens de forma a que uma entidade não autorizada não entenda o seu verdadeiro conteúdo. A primeira e principal garantia oferecida pela criptografia é a confidencialidade.

Quando uma entidade pretende enviar uma mensagem de forma confidencial, tem que a entregar ao algoritmo de encriptação de modo a que este a codifique numa mensagem encriptada. Na encriptação perfeita, não existe qualquer relação entre a mensagem encriptada e a original. Já no receptor, um algoritmo de desencriptação terá que gerar a mensagem original a partir da encriptada.

Os algoritmos de criptografia são de domínio público e bem conhecidos e, portanto, se tais algoritmos fossem

eficazes por si só para a encriptação e descriptação de mensagens, qualquer atacante poderia usá-los na descodificação não autorizada de mensagens da rede, quebrando por completo as características necessárias a um sistema seguro.

Desta forma, é necessária a utilização de sequências de bytes (geradas a partir de dados possivelmente aleatórios) nas operações de encriptação e descriptação, designadas por chaves. Assim, em caso de ataque, a entidade não autorizada só descodifica eficazmente a mensagem interceptada com a chave certa.

Em presença de chaves diferentes, o mesmo algoritmo de codificação/descodificação gera resultados diferentes, garantindo a reutilização do algoritmo criptográfico [3].

Num algoritmo de encriptação com chave perfeito, a mensagem encriptada não deve estar relacionada nem com o algoritmo de encriptação nem com a chave utilizada. Esta suposta ausência de relação entre mensagem por encriptar, mensagem encriptada e chave utilizada é fundamental, pois caso contrário seria possível recuperar a chave utilizada na encriptação a partir da mensagem encriptada, e proceder então à sua descriptação.

Nos algoritmos conhecidos existem essas relações, mas são de tal forma ténues que, dada a actual capacidade computacional, o tempo necessário para a geração de uma chave válida a partir de uma ou mais mensagens encriptadas pode ascender a centenas de anos.

Criptografia Simétrica

Num algoritmo de criptografia simétrica, os processos de encriptação e descriptação recorrem a uma mesma chave. Tipicamente, o emissor e o receptor partilham uma chave mantida em segredo a todo o custo.

Nomenclatura utilizada:

- Chave K :
- Mensagem: m
- Mensagem encriptada: m_k
- Função de codificação de uma mensagem m com chave K : $f(K, m) = K(m) = m_k$
- Função de descodificação de uma mensagem m_k com chave K : $f^{-1}(K, m_k) = K^{-1}(m_k) = m$

Suponhamos que as entidades e e r (respectivamente emissor e receptor) partilham uma chave simétrica K e pretendem trocar mensagens encriptadas (Figura 1). O emissor gera a mensagem encriptada a enviar (m_k) a partir da mensagem m e da chave K através do algoritmo de codificação:

$$m_k = K(m)$$

Na recepção, a entidade r descodifica a mensagem m_k utilizando a sua chave K através do algoritmo de

descodificação apropriado, recuperando assim a mensagem original:

$$m = K^{-1}(m_k)$$

Para esclarecer o mecanismo, consideremos a cifra de Caesar [3]. Esta cifra limita-se a deslocar cada letra do alfabeto n posições. Uma mensagem codificada com a cifra de Caesar utiliza uma chave K que corresponde ao número n : $K = n$.

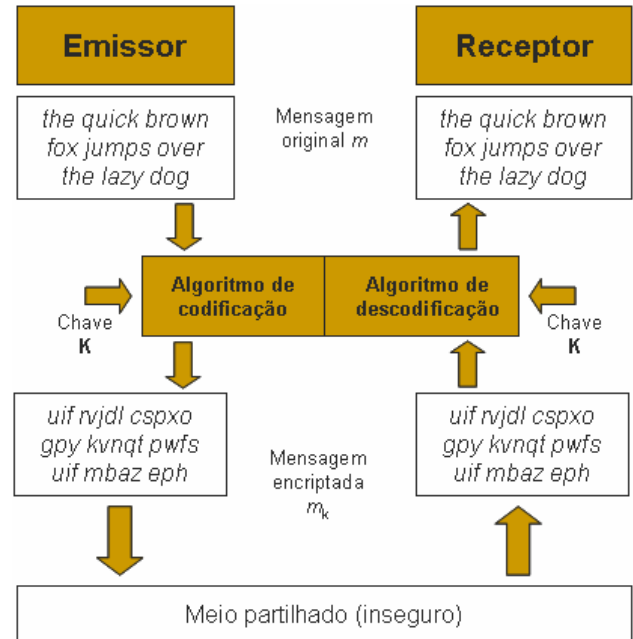


Figura 1 – Funcionamento de um algoritmo de criptografia simétrica. A mesma chave K é utilizada para encriptar e descriptar a mensagem. Note-se que os algoritmos de encriptação e descriptação podem ser iguais. Na cifra de Caesar, se $K=13$ não é preciso inverter o processo para descriptar – basta voltar a encriptar a mensagem encriptada para obter a versão original, ou seja, $f = f^{-1}$.

Por exemplo, considerando $n = 3$, uma mensagem $m = 'abc'$ será codificada em $'def'$:

$$m_k = K('abc') = 'def'$$

Para a descodificação, a chave é utilizada para produzir a operação inversa. A cifra de Caesar diz-se simétrica porque a mesma chave serve para codificar e descodificar a informação:

$$m = K^{-1}('def') = f^{-1}(K, m_k) = f(-K, m_k) = 'abc'$$

No entanto, para o emissor e o receptor terem a mesma chave secreta, é necessário que um deles gere a chave e depois a envie à outra entidade, o que, por sua vez, requer comunicação segura de forma a não comprometer a chave. Qualquer que seja a forma de distribuição da chave entre as entidades, esta é uma fase extremamente vulnerável, pois se alguém interceptar a chave pode então descodificar correctamente as mensagens trocadas entre o emissor e o receptor, perdendo-se novamente as características inerentes a um sistema seguro. A troca via

rede, sem mecanismos adicionais, está fora de questão pois qualquer entidade poderia interceptar a chave, e ficava automaticamente apta a descodificar as mensagens encriptadas.

Com um algoritmo de chave simétrica, toda e qualquer entidade que possua a chave pode enviar e receber correctamente mensagens encriptadas. A chave simétrica distribuída por mais do que uma entidade pode ser utilizada para uma forma rudimentar de difusão segura entre todas as entidades que possuem a chave.

Criptografia Assimétrica

O algoritmo *Diffie-Hellmann Key Exchange* [4] veio demonstrar a possibilidade de comunicação com encriptação sem a partilha prévia de uma chave secreta, através de um algoritmo elegante que deu origem aos actuais algoritmos usados na criptografia assimétrica, também conhecida como criptografia de chave pública [3].

A maior diferença entre os algoritmos de criptografia assimétrica e os utilizados na criptografia simétrica é o facto de que na criptografia assimétrica o processo de encriptação utiliza uma chave forçosamente diferente da chave utilizada na desencriptação.

Cada entidade possui um par de chaves: uma **chave pública** e uma **chave privada**.

A chave pública de uma entidade x é distribuída a todos os nós da rede, ou seja, a todas as outras entidades. Esta chave tem que ser pública para permitir o envio de informação encriptada das outras entidades para a entidade x . Por outro lado, a chave privada de x deve ser mantida secreta a todo o custo! O conhecimento da chave privada da entidade x compromete toda a informação encriptada que lhe possa ser enviada.

Nomenclatura utilizada:

- Chave pública: K^+
- Chave privada: K^-
- Chave da entidade e : K_e
- Chave pública da entidade e : K_e^+
- Chave privada da entidade e : K_e^-
- Mensagem: m
- Mensagem encriptada com chave K : m_k
- Função de codificação com chave K :
 $m_k = f(K, m) = K(m)$
- Função de descodificação com chave K :
 $m = f^{-1}(K, m_k) = K^{-1}(m_k)$
- Função de codificação de uma mensagem m com chave pública da entidade e :
 $m_{k_e^+} = f(K_e^+, m) = K_e^+(m)$

O algoritmo de chave pública pressupõe a existência de uma entidade emissora e , uma entidade receptora r e uma mensagem m . Além de cada entidade ter o seu par de chaves, pressupõe-se também que a entidade e tem a chave pública de r e a entidade r tem a chave pública de e . Resumindo, a entidade e tem os seguintes elementos:

- K_e^+ - a sua chave pública;
- K_e^- - a sua chave privada;
- m - a mensagem a enviar;
- K_r^+ - a chave pública da entidade r ;

Ao mesmo tempo, a entidade r tem em sua posse a seguinte informação:

- K_r^+ - a sua chave pública;
- K_r^- - a sua chave privada;
- K_e^+ - a chave pública da entidade e ;

A informação enviada para r é obtida através da encriptação de m utilizando a chave pública da entidade receptora r (Figura 2):

$$m_{k_r^+} = K_r^+(m)$$

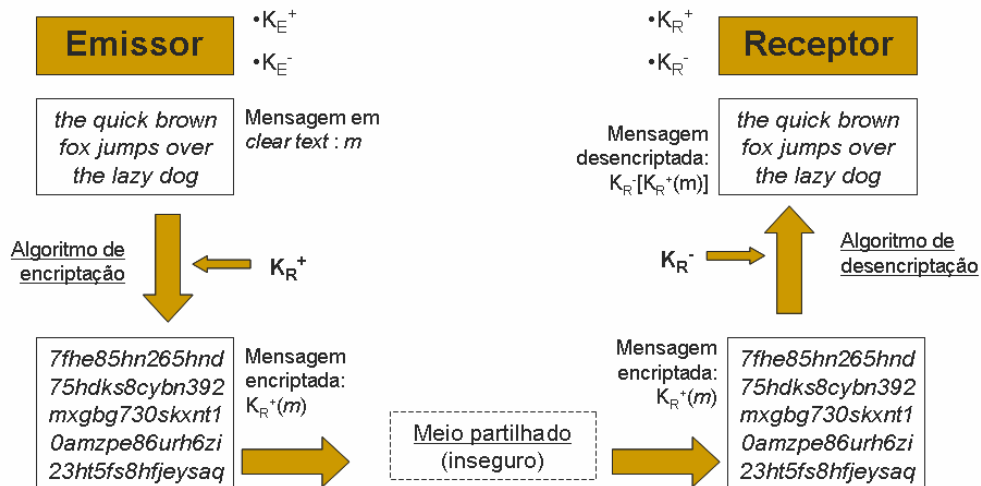


Figura 2 – Esquema básico do funcionamento da criptografia assimétrica.

Esta mensagem é enviada pela rede (de meio partilhado ou não) e, eventualmente, chegará à entidade receptora. Para recuperação da mensagem original, a entidade r descodifica a mensagem utilizando a sua chave privada:

$$m = K_r^- \left(K_r^+ (m_{k_r^+}) \right)$$

As entidades e e r referidas puderam assim comunicar seguramente (com confidencialidade) sem troca prévia de informação secreta. Em geral, qualquer entidade x que possua a chave pública de uma outra entidade y pode enviar-lhe mensagens encriptadas (confidenciais) com a certeza de que y as pode descodificar.

Propriedade fundamental da criptografia assimétrica:

$$K_z^- \left(K_z^+ (m) \right) = K_z^+ \left(K_z^- (m) \right) = m$$

$$f^{-1} \left(K^-, f \left(K^+, m \right) \right) = f^{-1} \left(K^+, f \left(K^-, m \right) \right) = m$$

Nota: f^{-1} pode ser igual a f .

Uma mensagem encriptada ($m_{k_x^+}$) com a chave pública da entidade x (K_x^+) pode apenas ser descriptada correctamente através da utilização da chave privada da mesma entidade x (K_x^-).

Ao mesmo tempo, uma mensagem encriptada ($m_{k_y^-}$) com a chave privada de uma entidade y (K_y^-) pode apenas ser recuperada através da descriptação com utilização da chave pública de y (K_y^+). Esta utilização descrita não serve como meio para atingir a confidencialidade, pois como K_y^+ é pública, a mensagem $m_{k_y^-}$ pode ser descriptada por todas as entidades que a possuam.

A reversibilidade dos algoritmos de criptografia assimétrica permite a sua exploração para além da confidencialidade.

Assinatura digital

A integridade das mensagens encriptadas trocadas entre entidades pode ser garantida através da utilização da criptografia assimétrica. A propriedade que confere esta possibilidade é a reversibilidade do algoritmo.

Supondo agora que e e r pretendem trocar mensagens não confidenciais mas com conteúdo que não possa ser alterado (total ou parcialmente). O emissor e envia a mensagem m com a sua identificação e uma verificação de integridade – cópia da mesma mensagem mas

encriptada com a sua chave privada ($m_{k_e^-}$). A mensagem enviada é então $m + m_{k_e^-}$. Todas as entidades da rede podem ver o conteúdo da primeira parte da mensagem (não vai encriptada) e, se pretenderem, podem também descodificar o conteúdo da segunda parte da mensagem, pois poderão ter em sua posse a chave pública da entidade e . Porém, apenas poderão concluir que a segunda parte da mensagem é uma cópia encriptada da primeira parte. O receptor r recebe a mensagem e começa por processar a descodificação da segunda parte da mensagem m_i ($m_i = K_e^+ (m_{k_e^-})$). A verificação da integridade é feita a partir da comparação de m com m_i . Se a mensagem não foi alterada, então ambas as partes são iguais. Caso tenha havido corrupção intencional ou accidental dos dados da mensagem, então as partes m e m_i não são iguais e r assume que a mensagem está corrompida.

A entidade emissora é a única capaz de processar a segunda parte da mensagem. Caso uma entidade x tente forjar uma mensagem, r vai descriptar a verificação com a chave pública de e e não de x , resultando m_i diferente de m .

Os processos de encriptação e descriptação são computacionalmente pesados e geram mensagens encriptadas tipicamente maiores em tamanho do que as mensagens por encriptar, proporcionando uma ineficiência adicional. O processo adoptado para minimizar esta ineficiência é a utilização de funções de *hash* na mensagem – *digests* (Figura 3).

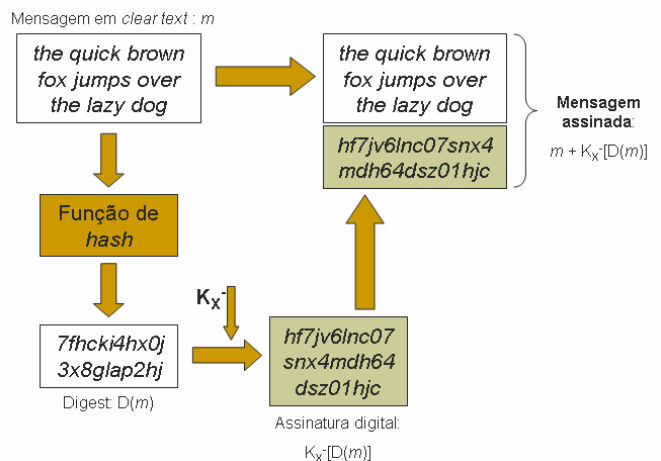


Figura 3 – Mecanismo de assinatura digital baseado em funções de *digest*. A mensagem assinada é composta pela concatenação da mensagem original com a encriptação do *digest* da mesma, utilizando a chave privada da entidade que gera a mensagem.

A função de *hash* calcula uma sequência de caracteres, geralmente de tamanho fixo, a partir da mensagem de comprimento arbitrário. O resultado deste cálculo é o *digest* $D(m)$ que protege a mensagem no sentido em que

se m se alterar (acidentalmente ou propositadamente) para m' , então $D(m')$ será forçosamente diferente de $D(m)$, possibilitando a detecção da alteração. Para garantir eficácia, o algoritmo de *hash* tem que ter as seguintes características:

- Facilidade computacional do cálculo de $D(m)$ dado m ;
- Função unidireccional (*one-way*). Não existe algoritmo inverso que permita calcular m a partir de $D(m)$ [1];
- Resistência de colisão fraca (*weak collision resistance*). Dada uma mensagem m e respectiva *hash* $D(m)$, é computacionalmente impossível encontrar m' diferente de m tal que $D(m) = D(m')$ [1];
- Resistência de colisão forte (*strong collision resistance*). Dada apenas a função de *hash* $D()$, é computacionalmente impossível encontrar duas mensagens diferentes m e m' de forma a que $D(m) = D(m')$ [1];

A assinatura digital é confirmada no receptor através do cálculo do *digest* da mensagem recebida e posterior comparação com a descodificação do *digest* recebido na assinatura (Figura 4).

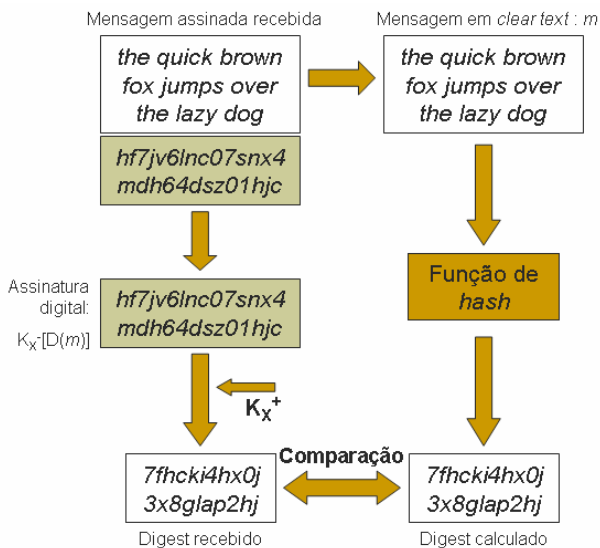


Figura 4 – Verificação de integridade. Comparação do *digest* calculado a partir da mensagem recebida com o *digest* recebido, calculado na fonte.

Naturalmente surge a combinação dos dois últimos mecanismos (assinatura digital e encriptação de mensagens) para gerar mensagens encriptadas e assinadas (Figura 5).

Através da utilização de algoritmos de *hash* eficazes, a verificação de integridade das mensagens é uma assinatura digital virtualmente impossível de falsificar, assumindo que nenhuma chave privada foi comprometida, e de cálculo eficiente, pois o *digest* é geralmente muito menor do que a mensagem a enviar.

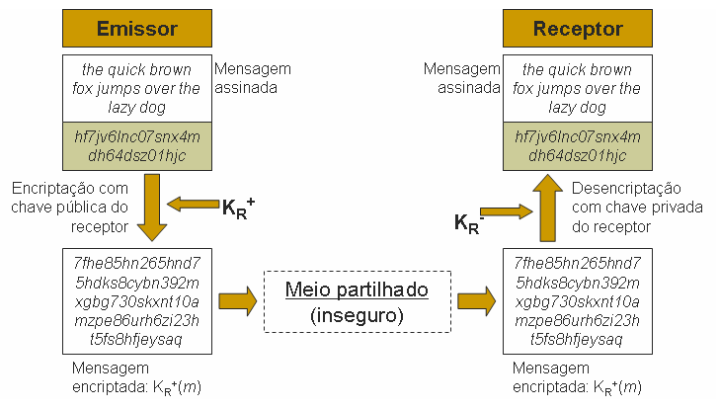


Figura 5 – Combinação dos métodos de encriptação de mensagens com algoritmo de cifra assimétrica e assinatura digital. O emissor encripta a mensagem m a enviar com a chave pública do receptor que depois a desencripta com a sua chave privada. Após a desencriptação, o receptor pode verificar a integridade da mensagem recebida como descrito na figura 4.

Certificação de chaves

Para a assinatura digital de mensagens foi assumido que a entidade que envia a mensagem diz ao receptor quem é, de forma a que o receptor saiba usar a respectiva chave pública para descodificar a assinatura digital.

De início, quando são trocadas as chave públicas entre o emissor e o receptor, a entidade x pode interceptar a chave pública de e e enviar a sua (K_x^+) a r . O receptor fica então na posse de uma chave pública que pensa ser de e mas que é de x . A este tipo de interceptação e substituição de mensagens por parte da entidade x , chama-se *man-in-the-middle*. A entidade x assume a identidade da entidade e , interceptando e substituindo as suas mensagens, sem que a entidade r se aperceba.

O problema óbvio que se põe é: como pode uma entidade ter a certeza de que uma outra entidade é quem diz ser? De forma a garantir o funcionamento regular e resistente a ataques é necessário que as entidades tenham a certeza que têm a chave pública da entidade com quem realmente estão a comunicar.

A forma de associar univocamente uma chave pública a uma entidade passa pela certificação da chave através de uma autoridade de certificação (*Certification Authority* – CA). O ataque do tipo *man-in-the-middle* torna-se assim ineficaz se as entidades utilizarem chaves públicas certificadas.

Uma entidade z dirige-se à autoridade com o intuito de certificar a sua chave pública. A autoridade verifica (pessoalmente, por exemplo) que a chave pública pertence à entidade em questão e gera um certificado digital que a associa à entidade. Esse certificado contém a chave pública da entidade z , a identificação de z (única) e uma assinatura digital da autoridade (figura 6).

O certificado é assinado digitalmente pela autoridade de forma a que não possa ser forjado ou alterado. Esta assinatura digital é do tipo referido acima, ou seja, a autoridade encripta o *digest* do certificado com a sua chave privada. Todas as entidades envolvidas em troca de mensagens cifradas ou assinaturas digitais devem conhecer e confiar na autoridade de certificação (ter acesso à sua chave pública), de forma a poderem verificar a validade do certificado.

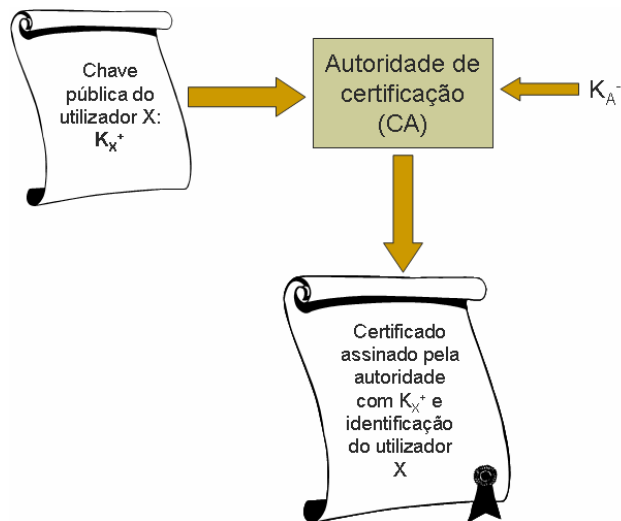


Figura 6 – Processo de certificação da chave pública da entidade x . A entidade que recebe o certificado entregue por x pode confirmar a sua autenticidade através da verificação da assinatura digital do certificado. Para conseguir esta verificação, é necessária a chave pública da autoridade de certificação, que deve ser facilmente obtida.

A interação de entidades com autoridades de certificação pressupõe confiança na autoridade, no sentido em que se acredita na rigorosa verificação da identificação da entidade e da chave pública. Por outras palavras, as entidades acreditam que o certificado é gerado com dados válidos, ou seja, que a associação chave pública / entidade é verdadeira.

Em última análise, uma chave pública certificada pode ser utilizada no âmbito da autorização, pois identifica univocamente a entidade que tenta aceder aos recursos de uma rede. O serviço que gere o recurso pode assim identificar a entidade em questão e comunicar com esta de forma segura (garantindo confidencialidade, integridade e autorização).

Conclusão

A criptografia assimétrica é uma ferramenta poderosa na segurança de um sistema distribuído. A sua utilização justifica-se claramente para a obtenção de confidencialidade, integridade e autorização. A confidencialidade é garantida através da criptografia forte, dependendo do algoritmo e da chave utilizada; a integridade passa pela utilização de assinaturas digitais; finalmente, uma autoridade de certificação (externa) permite estabelecer uma relação unívoca entre as

entidades e respectivas chaves públicas – certificação de chaves. O estabelecimento de sessões encriptadas com algoritmos de criptografia simétrica é feito de forma segura e elegante através da utilização da criptografia assimétrica.

Praticamente todos os dispositivos de segurança utilizados em redes de computadores utilizam criptografia assimétrica de forma directa ou em conjunto com outras técnicas de criptografia. Alguns exemplos mais conhecidos são:

- *Secure Shell* (ssh) para acesso remoto seguro;
- *PgP/GNUpg* (*Pretty good privacy/GNU privacy guard*) para troca de e-mails encriptados (utilização directa);
- *Secure Socket Layer* (SSL) *middleware*, que permitiu que aplicações ou protocolos que não foram concebidos a pensar na segurança pudessem ser facilmente alterados para comunicar de forma segura (utilização indirecta – compromisso entre algoritmos de criptografia simétrica e assimétrica). Por exemplo:
 - *HTTPs* (*Secure Hypertext Transfer Protocol*);
 - *IMAPs* (*Secure Internet Mail Access Protocol*);
 - *POPs* (*Secure Post Office Protocol*)
 - *sSMTP* (*Secure Simple Mail Transfer Protocol*)
- *Kerberos*, serviço de autenticação centralizado (utilização indirecta);

A utilização generalizada na Internet de protocolos envolvendo criptografia assimétrica promove e justifica o seu desenvolvimento.

Referências

- [1] Andrew S. Tanenbaum, M. van Steen, *Distributed Systems: Principles and paradigms* (Prentice-Hall, 2001).
 - [2] Thomas Y.C Woo, Simon S. Lam, Authentication for Distributed Systems, *IEEE Computer*, 25(1), 1992, 39-52.
 - [3] James F. Kurose, Keith W. Ross, *Computer Networking: a top down approach featuring the internet* (Addison Wesley 2003)
 - [4] W. Diffie, M. E. Hellmann, New directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, 1976, 644-654
- Peter Gutmann, PKI: It's Not Dead, Just Resting, *IEEE Computer*, 35(8), August 2002, 41-49.
- Patrick W. Dowd, John T. McHenry, Network Security: It's Time to Take It Seriously, *IEEE Computer*, 31(9), September 1998, 24-28.