Administração de Sistemas (ASIST)

Criptografia

Outubro de 2014

Criptografia – kryptós (escondido) + gráphein (escrita)

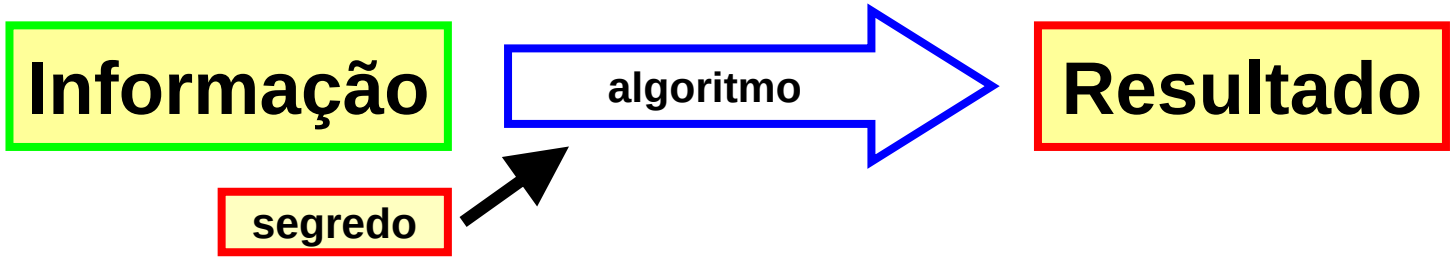
A criptografia utiliza algoritmos (funções) que recebem informação e produzem resultados que são úteis sob o ponto de vista de segurança.

Características de segurança que a criptografia ajuda a garantir

- **confidencialidade** – impossibilidade de leitura de dados por terceiros
- **integridade** – impossibilidade de alteração de dados por terceiros
- **autenticação** – impossibilidade de alguém se fazer passar por quem não é
- **não repúdio** – impossibilidade de alguém negar a autoria de algo

Chaves

Os algoritmos usados são do domínio público, a única forma de dificultar interferências de intrusos é inserir no processo algo que esse intruso desconhece.



Este segredo, normalmente designado de chave criptográfica ou chave secreta, influencia o resultado de tal forma que sem o conhecer o resultado perde a utilidade.

Uma chave secreta pode sempre ser descoberta, "basta" tentar todos os valores possíveis ("força bruta"). A segurança depende por isso do tamanho da chave, mas também de outros fatores.

Chave com mais bits → **Maior segurança**

A criptografia nunca dá total garantia de segurança

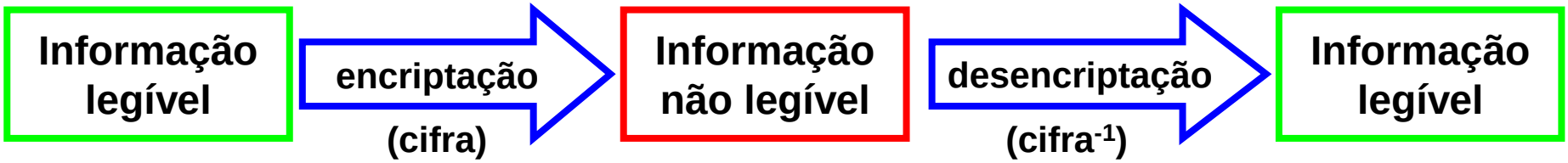
Confidencialidade

Uma forma de assegurar a confidencialidade é através do controlo de acesso:

- Lógico: o servidor verifica se o acesso de leitura deve ser autorizado
- Físico: colocando o recurso em local de acesso condicionado (ex.: cofre)

O controlo de acesso tem as suas vulnerabilidades e está sujeito a ataques, por isso pode não ser suficiente, além disso pode ser muito difícil de implementar como por exemplo nas comunicações em rede, em especial WAN.

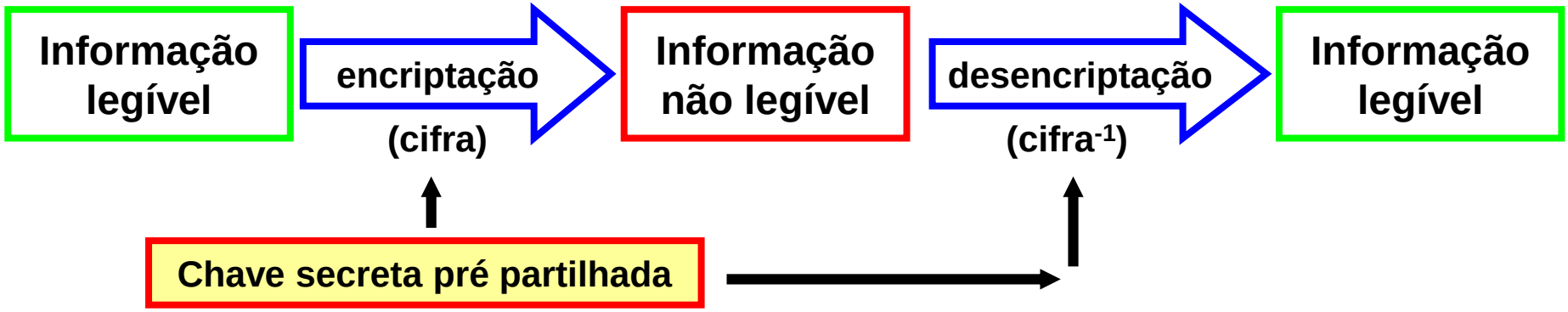
A criptografia fornece uma alternativa através dos algoritmos de cifra. São usados dois algoritmos complementares e inversos: encriptação e desencriptação.



Mesmo que haja acesso à informação, a confidencialidade está assegurada pelo facto de a informação não se encontrar numa forma legível.

Confidencialidade com cifras de chave simétrica

Também designada de "criptografia simétrica", de "chave pré-partilhada" ou de "chave secreta". Caraterizam-se por a mesma chave (secreta) ser usada na encriptação e na desencriptação.

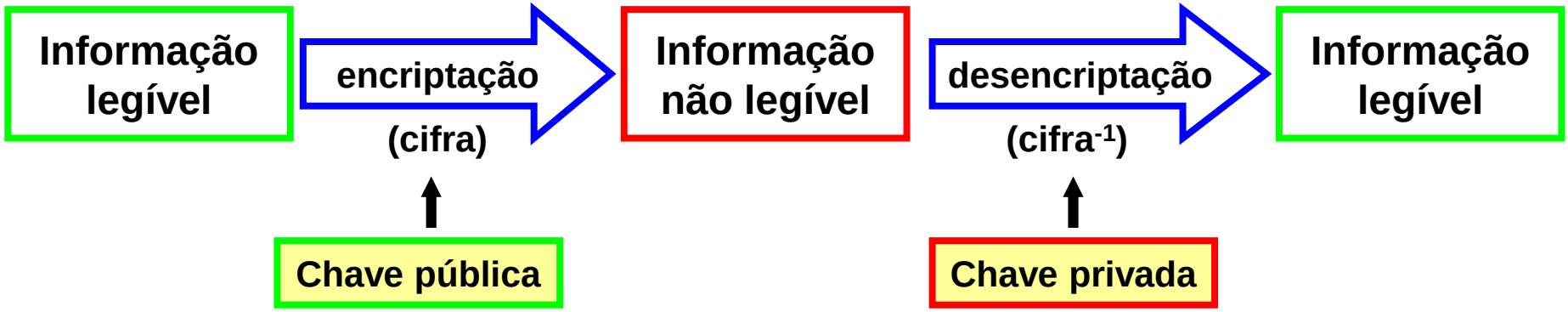


A chave secreta é conhecida apenas pelas duas entidades envolvidas na transação, por isso, além de assegurar a confidencialidade assegura também a autenticação e a integridade.

O grande problema deste tipo de cifras é a necessidade de haver um procedimento prévio de distribuição da chave que tem ele próprio de assegurar a confidencialidade e a autenticação.

Confidencialidade com cifras de chave assimétrica

Também designada de "criptografia de chave pública". Caraterizam-se por serem usadas duas chaves diferentes, uma para encriptação (chave pública) e outra para desencriptação (chave privada).

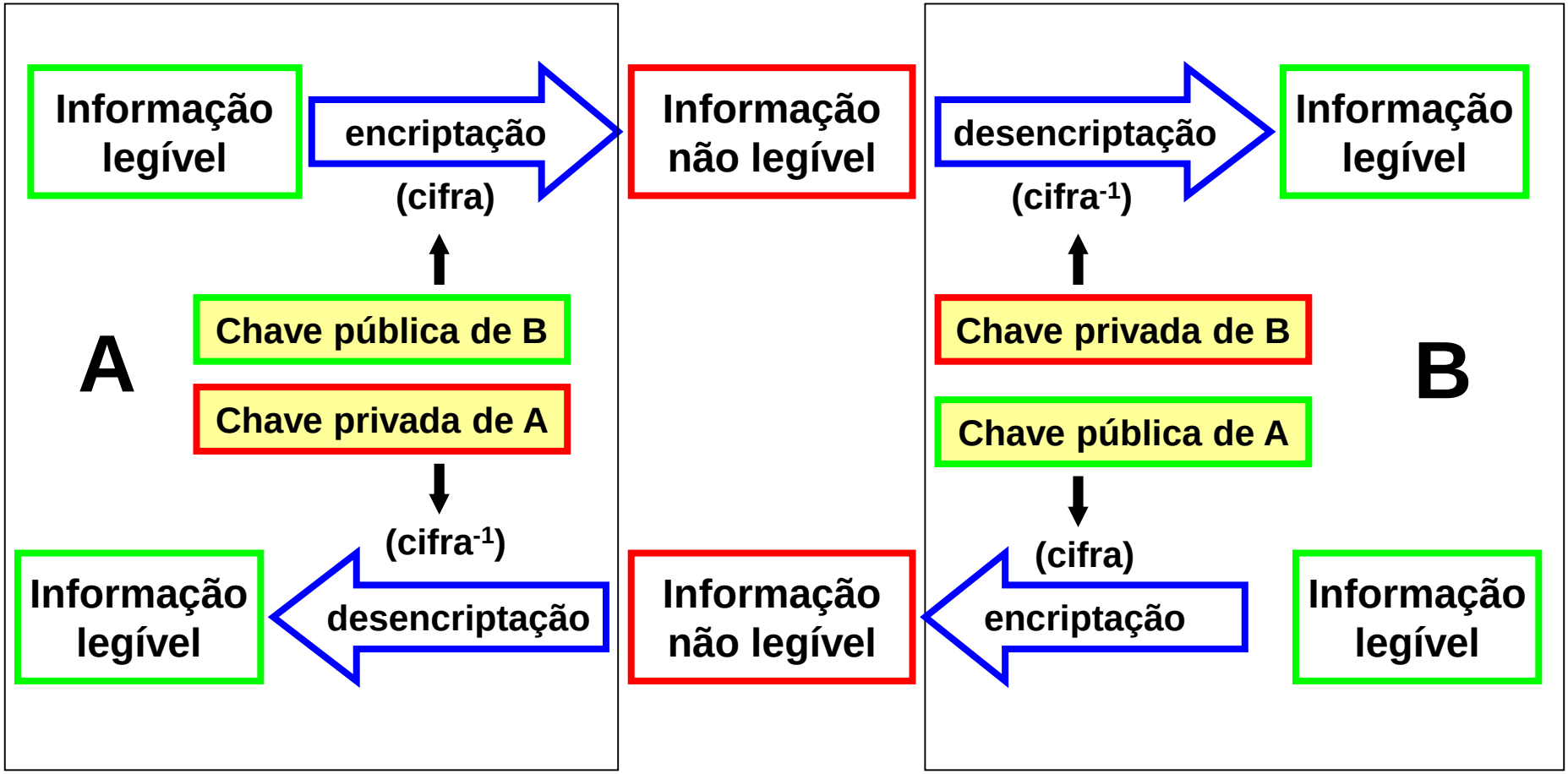


A chave pública é divulgada livremente, mas apenas serve para a encriptação, para a desencriptação é necessária a chave privada correspondente que é mantida secreta. Resolve parcialmente o problema da distribuição de chaves, mas tem outros inconvenientes.

Não é bidirecional porque um par de chaves apenas permite a confidencialidade num sentido.

Confidencialidade com cifras de chave assimétrica

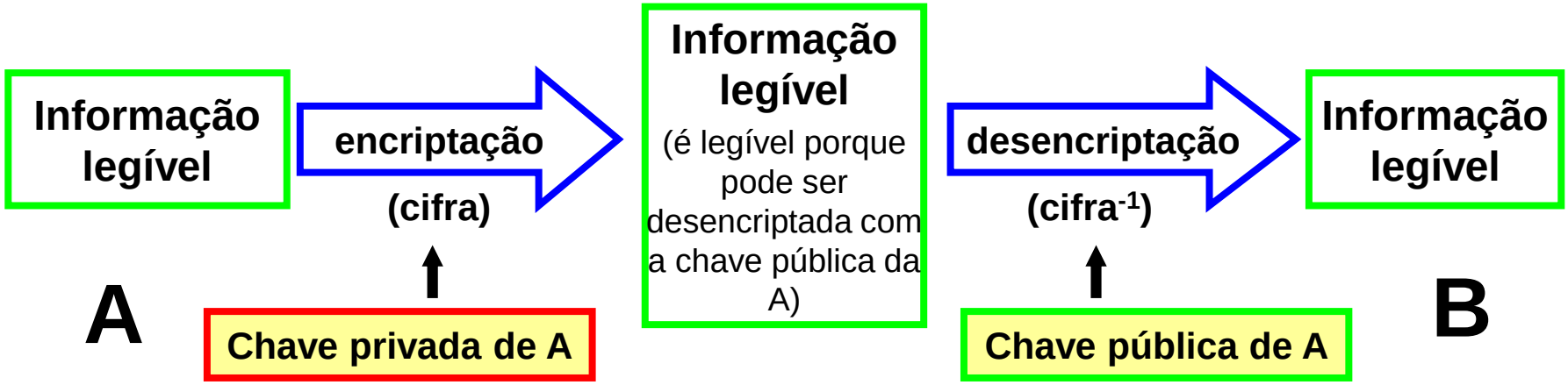
Um par "chave pública" / "chave privada" apenas assegura a confidencialidade num sentido, para a obter nos dois sentidos são necessários dois pares.



Autenticação com cifras de chave assimétrica

A utilização de uma chave pública facilita a distribuição de chaves, mas sob o ponto de vista do recetor não fornece qualquer garantia de autenticação (qualquer um pode produzir a mensagem encriptada usando a chave pública).

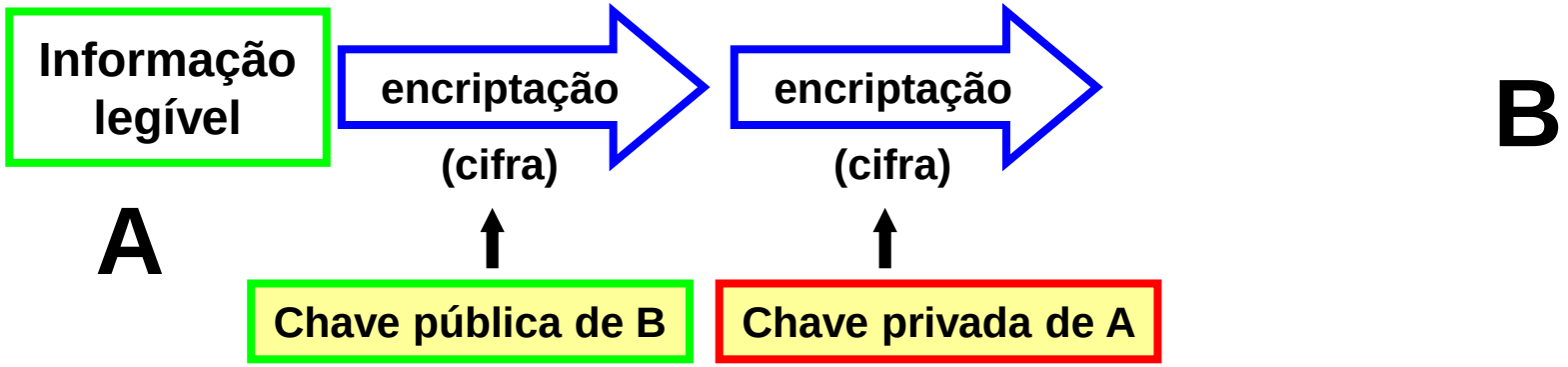
A autenticação pode ser obtida através de uma aplicação da cifra em forma invertida, usando a chave privada para encriptação e a chave pública para desencriptação. É claro que assim perde-se a confidencialidade.



Quando a entidade B recebe a informação tem garantias da sua origem e da sua integridade pois apenas a entidade A possui a "chave privada" correspondente à "chave pública de A". É ainda assegurado o "não repúdio".

Aplicação de cifras de chave assimétrica

Para garantir a confidencialidade e a autenticação/integridade/não repúdio simultaneamente são necessárias duas aplicações da cifra em cada um dos sentidos da transação.



A entidade B começa por realizar a desencriptação com a chave pública de A, isso assegura a autenticação/integridade/não repúdio, de seguida realiza a desencriptação com a sua chave privada assegurando a confidencialidade.

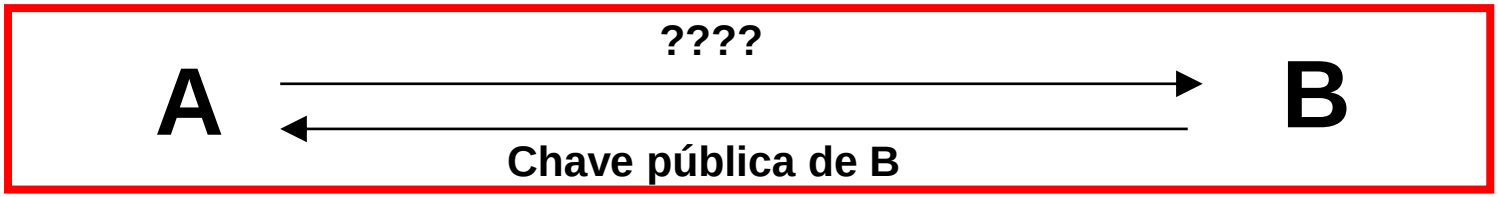
Todas estas garantias ficam comprometidas se as chaves públicas não forem distribuídas de forma adequada. Devido à sua conceção a distribuição não necessita de confidencialidade, mas necessita de autenticação.

Distribuição de chaves públicas

Toda a segurança das cifras assimétricas assenta sobre a autenticidade das chaves públicas.

Quando uma entidade A pretende garantir a confidencialidade num envio de dados a uma entidade B necessita da “chave pública de B”. Igualmente quando pretende ter garantias de autenticação/integridade/não repúdio sobre dados recebidos de B necessita da “chave pública de B”.

A entidade A não pode “pedir de forma arbitrária” à entidade B que lhe diga qual é a sua chave pública.

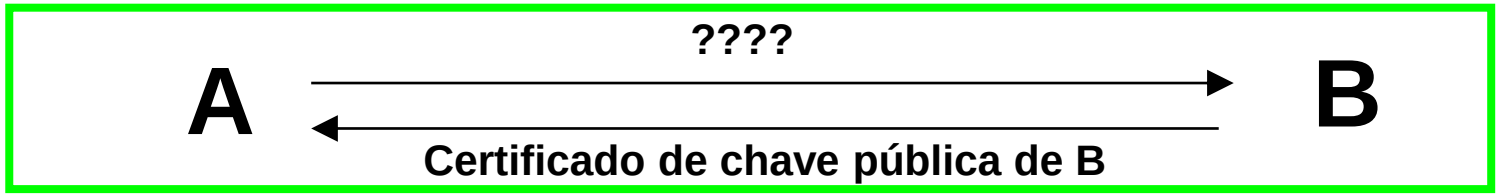


Um intruso poderia interferir na comunicação (“man-in-the-middle”) e fornecer uma chave pública falsa, permitindo-lhe desencriptar a informação enviada por A e também produzir informação que A aceitaria como sendo autentica e emitida por B.

Certificado de chave pública

O certificado de chave pública destina-se a garantir a autenticidade de uma chave pública é um documento digital legível que identifica o proprietário da chave, tipicamente através do nome DNS (fqdn), contém a chave pública e é assinado digitalmente por uma entidade certificadora de confiança.

A assinatura digital garante a autenticidade da associação entre o nome da entidade e a respetiva chave pública.



Quando A recebe o certificado verifica se está dentro do prazo de validade, verifica se o nome do proprietário (“owner”) corresponde ao que pretende contactar, verifica se o emissor (“issuer”) é uma entidade certificadora de confiança e valida a respectiva assinatura para garantir que o certificado é autentico.

Os certificados têm a vantagem de evitar a necessidade de contacto com a entidade certificadora para comprovar a autenticidade da chave pública.

Funções “hash”

As funções “hash” recebem um volume de informação indeterminado e produzem um resultado de tamanho fixo (alguns bytes), designado por “hash code”, “digest” ou “checksum”.

Sob o ponto de vista de criptografia, as suas carateristicas devem ser tais que o resultado representa o conteúdo da informação de entrada de uma forma dificilmente previsível, sendo por isso útil para validar a autenticidade e integridade dos dados.

Com uma função “hash” segura deve ser quase impossível:

- produzir pequenas alterações nos dados e ainda assim obter o mesmo resultado.
- encontrar duas mensagens diferentes que produzam o mesmo resultado

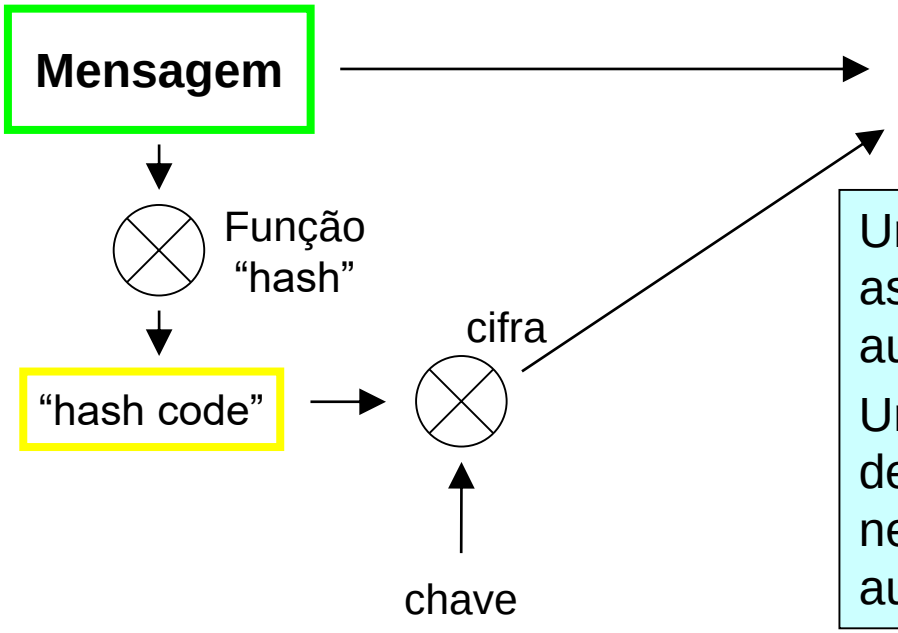
A aplicação assemelha-se a uma deteção de erros, o emissor envia a mensagem e o “hash”, o recetor calcula o “hash” da mensagem e confronta-o com o “hash” enviado para verificar se são iguais, atestando a integridade.

A grande diferença é que temos de prever ações maliciosas e não apenas erros aleatórios nas transmissões.

Funções “hash” em criptografia

A utilização de uma função “hash” não é suficiente para assegurar a integridade num ambiente hostil pois um intruso pode alterar a mensagem e recalcular o “hash code”.

Há necessidade de introduzir um elemento secreto desconhecido dos potenciais intrusos. Uma opção é simplesmente proceder a uma encriptação do “hash code”.



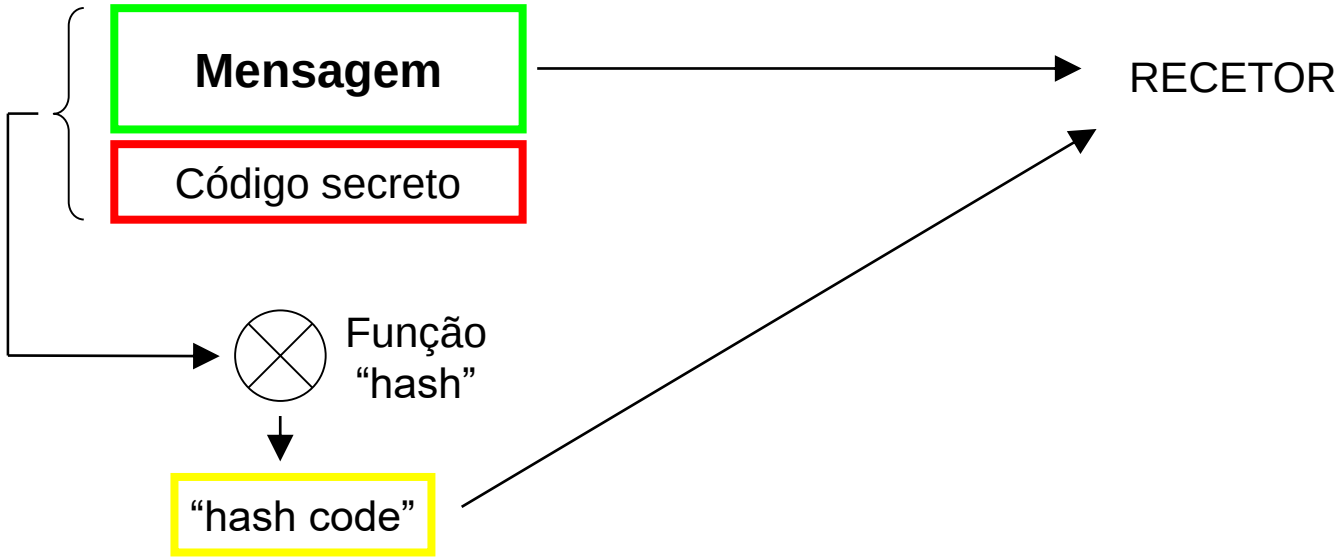
Uma cifra de chave simétrica vai assegurar a integridade e a autenticidade da mensagem.

Uma cifra de chave assimétrica terá de encriptar com a chave privada, neste caso assegura a integridade, autenticidade e não repúdio.

Funções “hash” criptográficas

São funções “hash” que recebem também um valor secreto que apenas é conhecido por emissor e recetor, assemelham-se por isso à aplicação de uma cifra de chave simétrica ao “hash code”. Estes “hash code” são por vezes designados de MAC (“Message Authentication Code”).

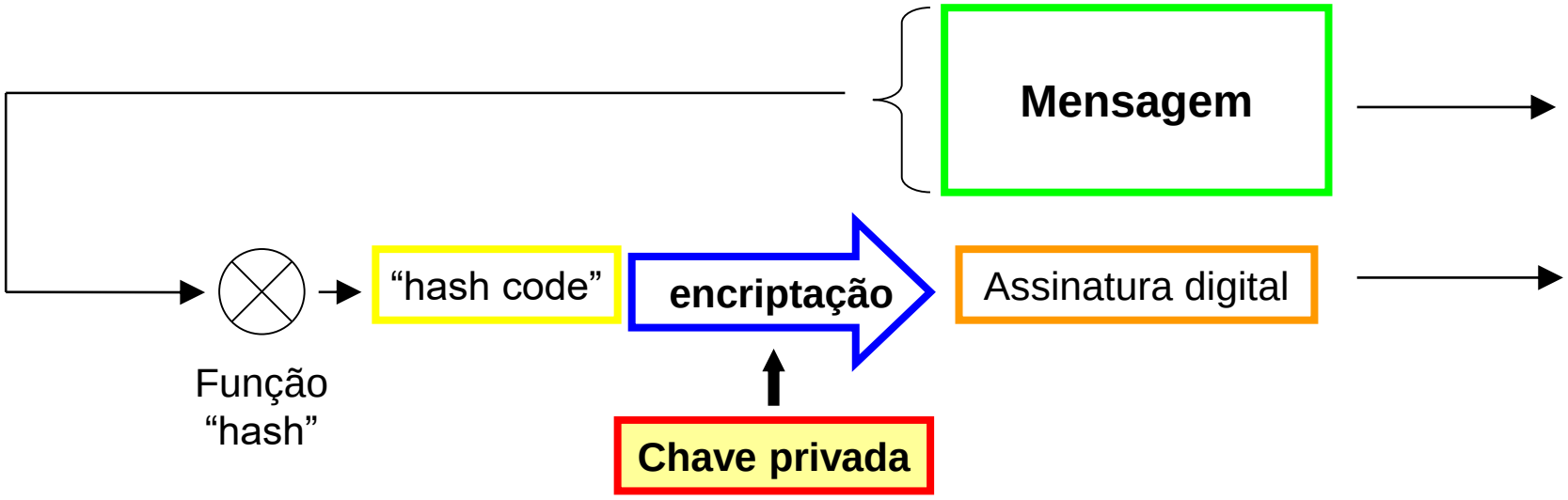
Uma forma simples de implementar consiste em combinar com o receptor um código secreto que é acrescentado à mensagem para cálculo do “hash-code”, mas nunca é transmitido.



Assinatura digital simples

A aplicação de encriptação assimétrica com a chave privada a um "hash-code" sólido permite implementar de uma forma simples todas as funcionalidades de uma assinatura digital, atestando:

- integridade do conteúdo
- autenticação do autor
- não repúdio (apenas o autor possui a chave privada)



Distribuição de chaves simétricas

A encriptação com cifras simétricas tem algumas vantagens sobre as cifras assimétricas, assegurando numa única aplicação a confidencialidade, autenticação e integridade, além disso são substancialmente mais rápidas do que as cifras assimétricas.

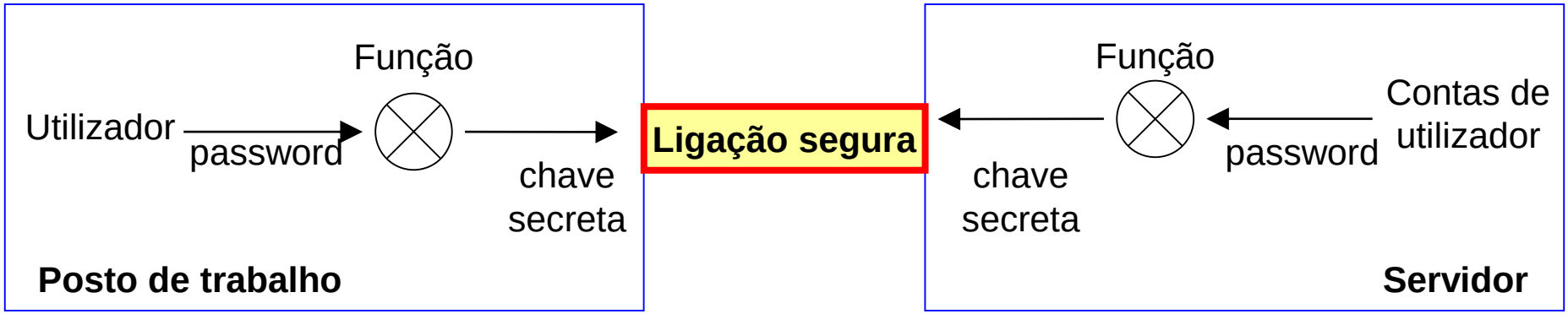
O seu maior problema encontra-se na distribuição de chaves que além da autenticação tem também de garantir a confidencialidade.

Numa ligação de caráter permanente entre dois dispositivos controlados por um mesmo administrador é relativamente simples colocar manualmente a mesma chave secreta nas duas extremidades. Quando se tratam de ligações dinâmicas, de curta duração, muitas vezes envolvendo utilizadores tudo se complica.

Uma solução é recorrer a um serviço de distribuição de chaves (KDC – Key Distribution Center), o sistema KERBEROS é um exemplo bastante usado, baseia-se na existência de uma chave pré-partilhada entre cada entidade e o KDC, sendo as chaves de sessão para comunicação entre entidades geradas pelo KDC e transmitidas às entidades de forma encriptada.

Distribuição de chaves simétricas por “password”

Uma outra alternativa, aplicável quando estão envolvidos utilizadores é usar as respectivas “passwords”, sendo esse um segredo que apenas é do conhecimento das duas entidades envolvidas, pode ser usado para produzir uma chave secreta em paralelo nas duas extremidades.



Este processo pode ser usado como mecanismo de autenticação de utilizadores sem transmissão da “password” e ser simultaneamente usado para gerar uma chave secreta nas duas extremidades.

A fraqueza da distribuição de chaves simétricas por “password” advém da fraqueza das “passwords” dos utilizadores pelo que deve ser associada a uma política de “passwords” exigente. Esta técnica é usada por exemplo nas VPNs do tipo PPTP.

Distribuição de chaves simétricas

As cifras de chave assimétrica são outra alternativa para distribuir chaves simétricas, sendo os certificados de chave pública um meio sólido se conseguir uma ligação segura, nada impede que essa ligação segura seja utilizada para enviar uma chave simétrica, abandonando de seguida a cifra de chave assimétrica:

1ª fase – as entidades A e B trocam entre si os respectivos certificados de chave pública e após validação estabelecem uma ligação segura usando uma cifra de chave assimétrica.

2ª fase – uma das entidades gera uma chave secreta de cifra simétrica e envia-a usando a ligação segura.

3ª fase – as entidades abandonam a cifra assimétrica e passam a usar a cifra simétrica com chave que foi gerada e transmitida.

Este método tem a vantagem de aliar a solidez da segurança da cifra assimétrica à melhor performance das cifras simétricas, é usado por exemplo no SSL/TLS.

Algoritmos “hash” - MD5 e SHA

O algoritmo MD5 (“Message-Digest 5”) recebe um bloco de dados de qualquer dimensão e produz um resultado de 128 bits, ainda é muito usado na actualidade, mas começa a ser considerado pouco seguro.

Um conjunto de algoritmos mais recente são os “Secure Hash Algorithm” (SHA):

Os algoritmos SHA-0 e SHA-1 produzem resultados de 160 bits, o segundo algoritmo corrige algumas fraquezas encontradas no anterior.

A designação SHA-2 representa um conjunto de algoritmos alternativos (SHA-224, SHA-256, SHA-384, SHA-512), cada um deles produz um resultado com o número de bits indicado na sua designação. Estas são consideradas algumas da alternativas mais sólidas na actualidade.

Actualmente encontra-se em fase final a competição para o SHA-3, deverá suportar resultados de 256 ou 512 bits, ou mesmo resultados de dimensão ajustável.

Cifras de chaves simétricas - DES

DES – “Data Encryption Standard”

Recebe blocos de 64 bits e encripta-os usando uma chave de 64 bits, a chave é constituída por 8 bytes, sendo um bit de cada um deles um bit de paridade, resultando por isso numa chave de 56 bits.

3DES – aplicação tripla do DES

Devido à reduzida dimensão da chave o DES simples não é considerado seguro, surgiram por isso aplicações múltiplas sucessivas do mesmo algoritmo, podendo ser usadas até 3 chaves distintas de 56 bits cada.

A aplicação dupla do DES poderia ser atacada através da técnica “meet-in-the-middle” o que levaria apenas ao dobro das tentativas relativamente ao DES simples.

Das várias versões existentes o 3DES mais flexível é o que recorre a duas encriptações com uma desencriptação intermédia.

Pode ser usado com 3 chaves diferentes, ou 2 chaves diferentes (K1=K3).

Se K1=K2, K2=K3 ou K1=K2=K3 torna-se equivalente a DES simples.

Cifras de chaves simétricas – RC2/RC4/RC5/RC6

Conjunto de algoritmos desenvolvidos por Ron Rivest designados de “Rivest Ciphers”, são bastante mais flexíveis do que o DES, nomeadamente através do suporte de chaves de tamanho variável que pode ser ajustado às necessidades crescentes.

RC2 (ARC2) – usa blocos de 64 bits com chave de comprimento configurável.

RC4 (ARC4) – recebe os dados em fluxo (não em blocos) e utiliza uma chave de comprimento configurável. Carateriza-se ainda por ser muito rápido, sendo usado por exemplo pelo WEP (“Wired Equivalent Privacy”).

RC5 – trabalha com blocos, mas é mais flexível podendo-se configurar o tamanho dos blocos, o tamanho das chaves e o número de iterações do algoritmo.

RC6 – algoritmo semelhante ao RC5 proposto para o concurso ao AES (“Advanced Encryption Standard”), sendo um dos cinco finalistas.

Embora todos estes algoritmos sejam flexíveis no tamanho das chaves, na actualidade considera-se que um mínimo de segurança se obtém com chaves de 128 bits (16 bytes), sendo já aconselhada a utilização de chaves de 256 bits para maior segurança.

Cifras de chaves simétricas – AES e outros

O IDEA (“International Data Encryption Algorithm”) usa blocos de 64 bits e uma chave de 128 bits. A chave de 128 bits pode ser considerada segura na atualidade.

O Blowfish usa blocos de 64 bits e uma chave flexível que pode ter de 32 até 448 bits.

O Twofish usa blocos de 128 bits e uma chave flexível que pode ter até 256 bits, foi um dos cinco finalistas ao concurso para o AES.

O AES (“Advanced Encryption Standard”) pretende ser o substituto do DES, usa blocos de 128 bits e uma chave de 128, 192 ou 256 bits.

Cifras de chaves assimétricas - RSA

O algoritmo RSA (“Ron Rivest, Adi Shamir e Leonard Adleman”) é um dos principais algoritmos de chave pública. Utiliza um problema matemático relacionado com a dificuldade em fatorizar números primos de grande dimensão.

A aplicação do algoritmo envolve cálculos com número de elevada dimensão e é por isso de execução morosa, as chaves podem ter comprimentos variáveis, tipicamente 512, 1024 ou 2048 bits.

O processo de geração de chaves também é complicado, tem como ponto de partida um conjunto de dois número primos de elevada dimensão que são por sí difíceis de determinar. O produto desses dois números designa-se por módulo (n).

As operações de encriptação e desencriptação são idênticas, apenas a chave (K) é diferente, no caso da encriptação usa-se a chave pública e na desencriptação a chave privada.

$$Y = X^K \bmod n$$

“mod” é o operador resto da divisão inteira

X deve ter uma ordem de grandeza pouco inferior a n

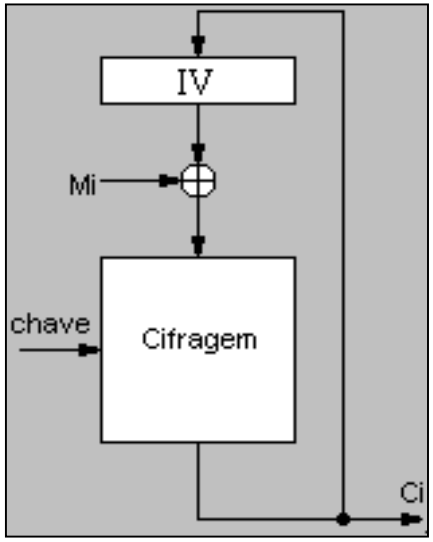
Aplicação de cifras de bloco

A aplicação das técnicas de cifra em bloco não deve facilitar os potenciais ataques, para isso é fundamental eliminar correspondências entre blocos de entrada e blocos cifrados.

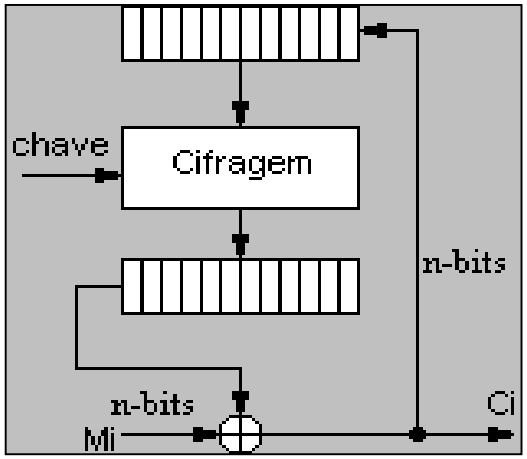
BLOCOS DE ENTRADA IGUAIS NÃO DEVEM PRODUZIR BLOCOS CIFRADOS IGUAIS

O problema é resolvido recorrendo a técnicas de realimentação em que o resultado da encriptação de um bloco depende dos anteriores, normalmente através de uma operação XOR. Na primeira iteração não existe um resultado anterior por isso usa-se um vetor inicial (IV).

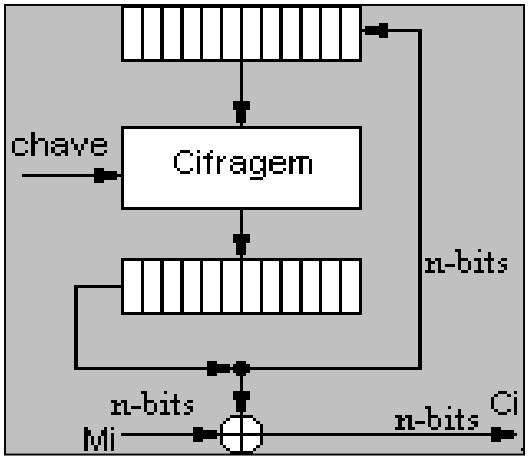
Cipher-block chaining (CBC)



Cipher feedback (CFB)



Output feedback (OFB)



Criptografia em rede

Os vários algoritmos descritos são aplicados nas várias camadas do modelo OSI através da sua inclusão em diversos protocolos, como por exemplo:

Camada de aplicação	**SSH; VPN**
Camada de transporte	**SSL/TLS**
Camada de rede	**IPSEC**
Camada de ligação lógica	**802.11i (WPA and WPA2)**

As implementações nas várias camadas não são mutuamente exclusivas, podendo mesmo ser usadas em conjunto para maior segurança.

Referências bibliográficas

[1] Lhamas A. (2010-2011). Aulas Teóricas de ASIST.

(…)