SERVIÇOS – AUTENTICAÇÃO E ASSINATURA DIGITAL

1

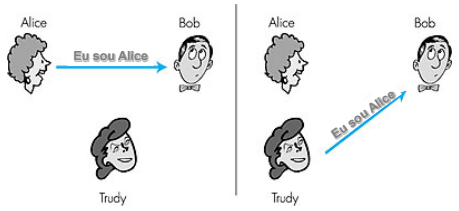
Criptografia – Serviços Oferecidos

Serviços	Descrição
Disponibilidade	Garante que uma informação estará disponível para acesso no momento desejado.
Integridade	Garante que o conteúdo da mensagem não foi alterado.
Controle de acesso	Garante que o conteúdo da mensagem será acessado somente por pessoas autorizadas.
Autenticidade da origem	Garante a identidade de quem está enviando a mensagem.
Não-repudiação	Previne que alguém negue o envio e/ou recebimento de uma mensagem.
Privacidade (confidencialidade ou sigilo)	Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento.

AUTENTICAÇÃO

Objetivo: Bob quer que Alice "prove" a sua identidade para ele

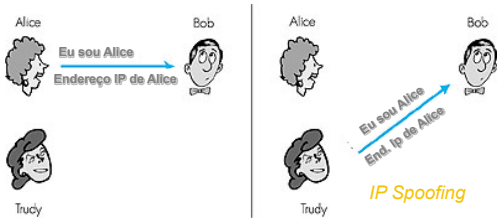
Protocolo ap1.0: Alice diz "Eu sou Alice"



3

AUTENTICAÇÃO: OUTRA TENTATIVA

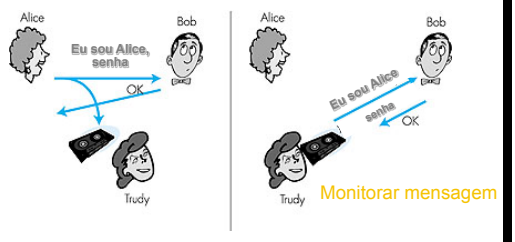
Protocolo ap2.0: Alice diz "Eu sou Alice" e envia junto o seu endereço IP como "prova".



4

AUTENTICAÇÃO: OUTRA TENTATIVA

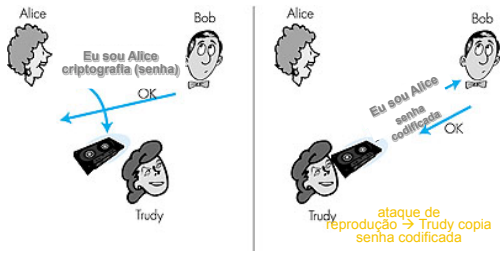
Protocolo ap3.0: Alice diz "Eu sou Alice" e envia a sua senha secreta como "prova".



5

AUTENTICAÇÃO: AINDA UMA OUTRA TENTATIVA

Protocolo ap3.1: Alice diz "Eu sou Alice" e envia a sua senha secreta *codificada* como "prova".



6

AUTENTICAÇÃO: AINDA UMA OUTRA TENTATIVA

Objetivo: evitar ataque de reprodução (*playback*)

Nonce: número (R) usado apenas uma vez

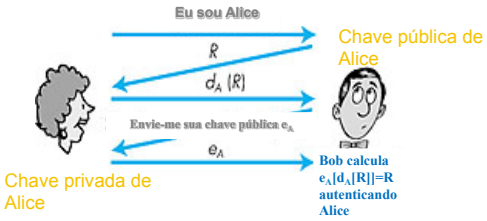
ap4.0: de modo a identificar Alice "ao vivo", Bob envia para Alice um ***nonce*** R, Alice deve retornar R codificado com a chave simétrica

Chave simétrica deve ser compartilhada

7

AUTENTICAÇÃO: AP5.0

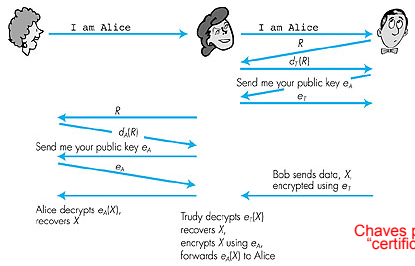
ap5.0: usar *nonce*, criptografia de chave pública



8

AP5.0: BRECHA DE SEGURANÇA

***man-in-the-middle*: Trudy se passa por Alice (para Bob) e por Bob (para Alice)**



9

CRIPTOGRAFIA SIMÉTRICA *X* ASSIMÉTRICA

Número de chaves necessárias/número de participantes

Nº de participantes	Criptografia Simétrica $n(n-1)/2$	Criptografia Assimétrica $2n$
2	1	4
4	6	8
8	28	16
16	120	32

10

CRIPTOGRAFIA SIMÉTRICA *X* ASSIMÉTRICA

Simétrica	Assimétrica
Funcionamento ○ Utiliza um algoritmo e uma chave para cifrar e decifrar	**Funcionamento** ○ Utiliza um algoritmo e um par de chaves para cifrar e decifrar
Requisito de Segurança ○ A chave tem que ser mantida em segredo ○ Tem que ser impossível decifrar a mensagem ○ Algoritmo mais alguma parte do texto cifrado devem ser insuficientes para obter a chave	**Requisito de Segurança** ○ Uma chave é pública e a outra tem que ser mantida em segredo ○ Algoritmo com alguma parte do texto cifrado com uma das chaves não devem ser suficientes para obter a outra chave

11

CRIPTOGRAFIA SIMÉTRICA *X* ASSIMÉTRICA

Problemas

Criptografia Simétrica

- Como distribuir e armazenar as chaves secretas de forma segura?
- Quantas chaves são necessárias para uma comunicação segura entre *n* pessoas?

Criptografia Assimétrica

- Como garantir que o detentor da chave pública é realmente quem diz ser?
- Necessidade de ter uma infra-estrutura para armazenar as chaves públicas.

12

CRIPTOGRAFIA - AUTENTICAÇÃO

- Algumas vezes há a necessidade de se provar quem escreveu um documento e de manter as informações desse documento sem modificações.
- **Solução**: serviços de autenticação e integridade de dados

A autenticidade de muitos documentos é determinada pela presença de uma **Assinatura Digital**.

13

CRIPTOGRAFIA - AUTENTICAÇÃO

- **Assinatura digital** – item que acompanha um determinado dado e apresenta as seguintes funções:
  1. Confirmar a origem do dado
  2. Certificar que o dado não foi modificado
  3. Impedir a negação de origem

14

ASSINATURA DIGITAL

- Vantagens provenientes do envio de mensagem "**assinada**":
  1. O receptor poderá verificar a identidade alegada pelo transmissor.
  2. Posteriormente, o transmissor não poderá repudiar o conteúdo da mensagem.
  3. O receptor não terá a possibilidade de forjar ele mesmo a mensagem.

15

ASSINATURA DIGITAL

- Assinaturas de Chave Simétrica
- Assinaturas de Chave Pública
- Sumários de mensagens (*Message Digests*)
- Aplicações Práticas

16

ASSINATURA DIGITAL

Assinatura de Chave Simétrica

Estratégia – uso de uma autoridade central que saiba de tudo e na qual todos confiem (BB - *Big Brother*).

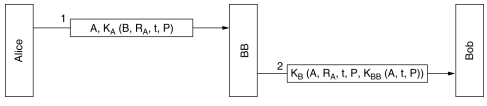
Cada usuário escolhe uma chave secreta e a leva para o BB.

Somente Alice e BB conhecem a chave secreta de Alice, K_A, e assim por diante.

17

ASSINATURA DIGITAL

Assinatura de Chave Simétrica



Assinaturas digitais com *Big Brother*

B – identidade de Bob
R_A – número aleatório escolhido por Alice
t – timbre de hora para assegurar a atualidade
$K_A(B, R_A, t, P)$ – mensagem criptografada com a chave de Alice, K_A
$K_{BB}(A, t, P)$ – mensagem assinada

18

ASSINATURA DIGITAL

Problemas - Assinaturas de Chave Simétrica

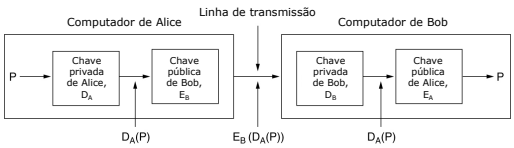
Todos têm de confiar no BB.

O BB tem de ler todas as mensagens assinadas.

19

ASSINATURA DIGITAL

Assinaturas de Chave Pública



Assinaturas digitais com o uso de chave pública.

20

ASSINATURA DIGITAL

Assinaturas de Chave Pública - Problemas relacionados ao ambiente no qual operam

- Bob só poderá provar que uma mensagem foi enviada por Alice enquanto D_A permanecer secreta. Se Alice revelar sua chave secreta, o argumento deixará de existir - qualquer um poderá ter enviado a mensagem.
- **O que acontecerá se Alice decidir alterar sua chave?**

21

ASSINATURA DIGITAL

Criptografia Assimétrica (chave pública) - Críticas

Reúnem sigilo e autenticação

Em geral, o sigilo não é necessário

Cifragem da mensagem inteira é lenta

Solução:
assinar a mensagem sem cifrá-la completamente

Sumários de Mensagens

22

ASSINATURA DIGITAL

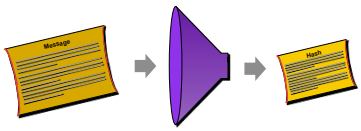
Sumários de Mensagens (*Message Digests*)

- Uso de uma **função *hash*** unidirecional que extrai um trecho qualquer do texto simples e, a partir deste, calcula um *string* de bits de tamanho fixo.
- **Função hash** – geralmente denominada **sumário de mensagens** (MD).

23

ASSINATURA DIGITAL

•Hash - Algoritmo que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor, de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash.



Função Hash - funciona como uma **impressão digital de uma mensagem** gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno: o **digest** ou **valor hash**.

24

ASSINATURA DIGITAL

MD - Propriedades importantes

1. Se ***P*** **for fornecido, o cálculo de *MD*(*P*) será muito fácil.**
2. **Se *MD*(*P*) for fornecido, será efetivamente impossível encontrar *P*.**
3. **Dado *P*, não deve ser possível encontrar *P´* tal que *MD*(*P´*) = *MD*(*P*).**
4. **Uma mudança na entrada de até mesmo 1 bit produz uma saída muito diferente.**

25

ASSINATURA DIGITAL

Message Digests - Propriedades importantes

Gera um sumário de tamanho fixo para qualquer comprimento de mensagem.

Efetivamente impossível adivinhar a mensagem a partir do sumário.

Efetivamente impossível encontrar outra mensagem que gere o mesmo sumário.

Uma pequena mudança na mensagem altera bastante o sumário.

26

FUNÇÃO HASH – *MESSAGE DIGESTS*

Assinando o HASH pode-se garantir estar assinando o próprio documento original pois cada HASH é único

27

ASSINATURA DIGITAL

Exemplos de algoritmos que implementam Assinatura Digital:

- **RSA**
- **El Gamal**
- **DSA**

28

ASSINATURA DIGITAL

Algoritmo	Descrição
RSA	•Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. •A matemática é a mesma: há uma chave pública e uma chave privada, e a segurança do sistema baseia-se na **dificuldade da fatoração de números grandes**.

29

ASSINATURA DIGITAL

Algoritmo	Descrição
El Gamal	•Também é comutativo, podendo ser utilizado tanto para assinatura digital quanto para gerenciamento de chaves. •Obtém sua segurança da dificuldade do cálculo de **logaritmos discretos** em um corpo finito.

30

ASSINATURA DIGITAL

Algoritmo	Descrição
DSA	•O *Digital Signature Algorithm*, **destinado unicamente a assinaturas digitais**, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (*Digital Signature Standard*). •Adotado como padrão final em dezembro de 1994, trata-se de uma variação dos algoritmos de assinatura El Gamal e Schnorr.

31

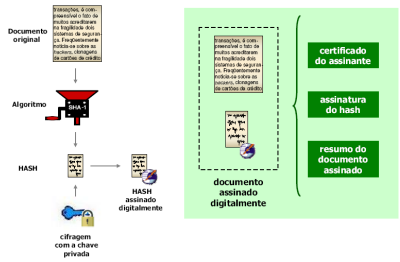
CRIPTOGRAFIA - FUNÇÃO HASH

Exemplos de funções *hash (MD)* utilizadas em produtos e protocolos criptográficos:

- **MD5**
- **SHA-1**
- **MD2 e MD4**

32

ASSINATURA DIGITAL - GERAÇÃO



33

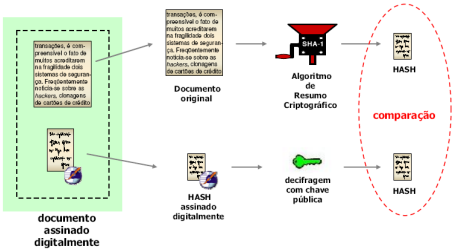
ASSINATURA DIGITAL - GERAÇÃO

Geração da Assinatura Digital

1. entra-se com os dados a serem "digeridos" e o algoritmo MD gera um *hash* de 128 ou 160 bits (dependendo do algoritmo).
2. computada uma *MD*, criptografa-se o *hash* gerado com uma chave privada.

34

ASSINATURA DIGITAL - VERIFICAÇÃO



Normalmente, $2^{m/2}$ (e não 2^m) operações são suficientes para subverter um sumário de mensagens de m bits utilizando-se o **ataque de aniversário**.

35

ASSINATURA DIGITAL - VERIFICAÇÃO

Verificação da Assinatura Digital

1. Executa-se a função MD (usando o mesmo algoritmo MD que foi aplicado ao documento na origem), obtendo-se um *hash* para aquele documento, e posteriormente, decifra-se a assinatura digital com a chave pública do remetente.
2. A assinatura digital decifrada deve produzir o mesmo *hash* gerado pela função MD executada anteriormente.
3. Se estes valores são iguais é determinado que o documento não foi modificado após a assinatura do mesmo, caso contrário o documento ou a assinatura, ou ambos foram alterados.

Assinatura digital – informa apenas que o documento foi modificado, mas não o que foi modificado e o quanto foi modificado.

36

ASSINATURA DIGITAL

É importante perceber: a assinatura digital, como descrita no exemplo anterior, não garante a confidencialidade da mensagem.

Qualquer um poderá acessá-la e verificá-la, mesmo um intruso (*Eva*), apenas utilizando a chave pública de *Alice*.

37

ASSINATURA DIGITAL

Obtenção de confidencialidade com assinatura digital:

- **Alice**
  1. assina a mensagem, utilizando sua chave privada.
  2. criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública de Bob.
- **Bob**
  1. ao receber a mensagem, deve decifrá-la com sua chave privada, o que garante sua privacidade.
  2. "decifrá-la" novamente, ou seja, verificar sua assinatura utilizando a chave pública de Alice, garantindo assim sua autenticidade.

38

ASSINATURAS DIGITAIS - RESUMO

Técnica criptográfica análoga às assinaturas à mão

Transmissor (Bob) assina digitalmente o documento, atestando que ele é o dono/ criador do documento

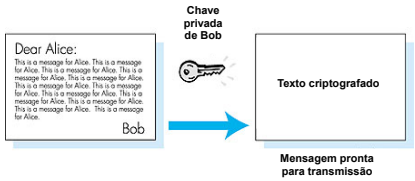
Verificável, não falsificável e incontestável (irretratabilidade): destinatário (Alice) pode verificar que Bob, e ninguém mais, assinou o documento

39

ASSINATURAS DIGITAIS

Assinatura digital simples para a mensagem m:

- **Bob codifica m com a sua chave privada d_B, criando a mensagem assinada, $d_B(m)$**
- **Bob envia *m* e $d_B(m)$ para Alice**



ASSINATURAS DIGITAIS

Suponha que Alice receba a mensagem *m*, e a assinatura digital $d_B(m)$

Alice verifica que *m* foi assinada por Bob por meio da aplicação da chave pública dele e_B à $d_B(m)$, e checa se

$e_B(d_B(m)) = m$

Se $e_B(d_B(m)) = m$, quem quer que tenha assinado *m* deve ter usado a chave privada de Bob

Alice portanto verifica que:

- Bob assinou *m*
- Ninguém mais assinou *m*
- Bob assinou m e não *m'*

Irretratabilidade:

- Alice pode levar *m*, e a assinatura $d_B(m)$ para um tribunal, por exemplo, e provar que Bob assinou *m*

41

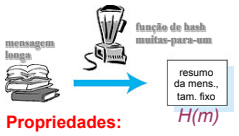
RESUMO (*DIGEST*) DE MENSAGENS

A codificação com chave pública de mensagens longas é cara computacionalmente

Objetivo: assinatura digital (impressão digital) de comprimento fixo, fácil de ser calculada

aplique função *hash* H a m

- obtém resumo da mensagem de comprimento fixo, *H(m)*



Propriedades:

Muitas-para-um

Produz resumo da mensagem de comprimento fixo

Dado o resumo da mensagem x é computacionalmente inviável encontrar m de modo que

x = H(m)

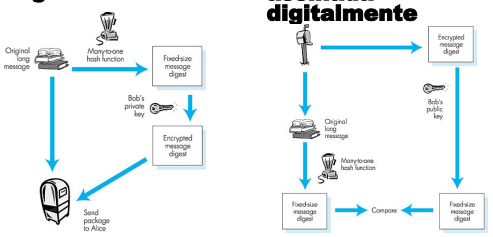
é computacionalmente inviável encontrar duas mensagens m e m' tais que *H(m) = H(m')*

42

ASSINATURA DIGITAL = ASSINATURA DO RESUMO DA MENSAGEM

Bob envia mensagem assinada digitalmente

Alice verifica a assinatura e a integridade da mensagem assinada digitalmente



43

SEGURANÇA NA INTERNET

Função Hashing

A assinatura digital obtida através do uso da **criptografia assimétrica** ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, do modo como foi didaticamente descrito no item anterior. Está faltando, portanto, descrever um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função Hashing. Sua utilização como componente de assinaturas digitais se faz necessário devido à lentidão dos algoritmos assimétricos, em geral cerca de 1.000 vezes mais lentos do que os simétricos.

Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente "cifradas" com a chave privada de alguém. Ao invés disso, é empregada uma função Hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho. Assim, a função Hashing oferece agilidade nas assinaturas digitais, além de integridade confiável, conforme descrito a seguir.

44

SEGURANÇA NA INTERNET

Função Hashing

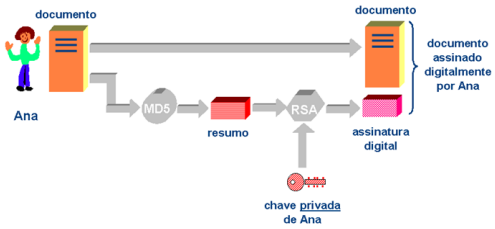
Também denominada Message Digest, One-Way Hash Function, Função de Condensação ou Função de Espalhamento Unidirecional, a função Hashing funciona como uma impressão digital de uma mensagem gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno: o digest ou valor hash.

Este valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta-corrente está para o número da conta ou o check sum está para os valores que valida. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa. Assim, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação em seu conteúdo -mesmo em apenas um bit da mensagem - será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto.

45

SEGURANÇA NA INTERNET

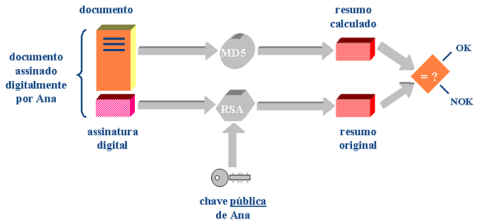
Função Hashing



46

SEGURANÇA NA INTERNET

Função Hashing



47

SEGURANÇA NA INTERNET

Função Hashing

Funções	Descrição
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa Message Digest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função Hashing prévia de Rivest: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor hash de somente 128 bits é o que causa maior preocupação; é preferível uma função Hashing que produza um valor maior.
SHA-1	O Secure Hash Algorithm, uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte do MD5, citada anteriormente, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Atualmente, não há nenhum ataque de criptoanálise conhecido contra o SHA-1. Mesmo o ataque da força bruta torna-se impraticável, devido ao seu valor hash de 160 bits. Porém, não há provas de que, no futuro, alguém não possa descobrir como quebrar o SHA-1.

48

SEGURANÇA NA INTERNET

Função Hashing

MD2 e MD4	O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um hash de 128 bits. A segurança do MD2 é dependente de uma permutação aleatória de bytes. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções hash citadas e acredita-se que seja menos seguro.

SEGURANÇA NA INTERNET

Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (info)	Example performance[2] (MiB/s)	First Published
MD5 (as reference)		128	128 (4 × 32)	512	Unlimited[3]	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	335	1992
SHA-0		160	160 (5 × 32)	512	$2^{64}-1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<80 (collisions found)	-	1993
SHA-1		160	160 (5 × 32)	512	$2^{64}-1$	80		<63 (collision found[4])	192	1995
SHA-2	*SHA-224*	224	256 (8 × 32)	512	$2^{64}-1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112	139	2001
	SHA-256	256						128		
	SHA-384	384	512 (8 × 64)	1024	$2^{128}-1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192	154	2001
	SHA-512	512						256		
	SHA-512/224	224						112		
	SHA-512/256	256						128		
SHA-3	*SHA3-224*	224	1600 (5 × 5 × 64)	1152	Unlimited[5]	24[6]	And, Xor, Rot, Not	112	-	2015
	SHA3-256	256		1088				128		
	SHA3-384	384		832				192		
	SHA3-512	512		576				256		
	SHAKE128	*d* (arbitrary)		1344				min(*d*/2, 128)	-	2015
	SHAKE256	*d* (arbitrary)		1088				min(*d*/2, 256)		

SEGURANÇA NA INTERNET

Obtendo uma Assinatura Digital

Um certificado digital é um documento eletrônico que contém as informações da identificação de uma pessoa ou de uma instituição. Esse documento deve ser solicitado a uma AC ou ainda a uma AR (**A**utoridade de **R**egistro). Uma AR tem a função de solicitar certificados a uma AC.

Para que um certificado seja válido, é necessário que o interessado tenha a chave pública da AC para comprovar que aquele certificado foi, de fato, emitido por ela. A questão é que existem inúmeras ACs espalhadas pelo mundo e fica, portanto, inviável ter a chave pública de cada uma.

A solução encontrada para esse problema foi a criação de "ACs supremas" (ou "ACs-Raiz"), ou seja, instituições que autorizam as operações das ACs que emitem certificados a pessoas e empresas. Esse esquema é conhecido como ICP (**I**nfra-estrutura de **C**haves **P**úblicas) ou, em inglês, PKI (**P**ublic **K**ey **I**nfrastructure).

SEGURANÇA NA INTERNET

Obtendo uma Assinatura Digital

No Brasil, a ICP-Brasil controla seis ACs: a Presidência da República, a Receita Federal, o SERPRO, a Caixa Econômica Federal, a Serasa e a CertiSign. Isso significa que, para que tenha valor legal diante do governo brasileiro, uma dessas instituições deve prover o certificado. Porém, para que isso seja feito, cada instituição pode ter requisitos e custos diferentes para a emissão, uma vez que cada entidade pode emitir certificados para finalidades distintas. E isso se aplica a qualquer AC no mundo.

Agora, uma coisa que você deve saber é que qualquer instituição pode criar uma ICP, independente de seu porte. Por exemplo, se uma empresa criou uma política de uso de certificados digitais para a troca de informações entre a matriz e sua filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP-Brasil. A própria empresa pode criar sua ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

CHAVES SIMÉTRICAS VS ASSIMÉTRICAS

Vantagens das chaves simétricas:

- **Desempenho, são rápidos**

Vantagens das chaves assimétricas:

Facilidade de distribuição de chaves
Permitem:
- assinaturas
- certificados digitais

Apenas uma chave para todas as aplicações

UM EXERCÍCIO ...

Duas pessoas (um remetente e um receptor) têm uma mensagem (documento).

A mensagem do receptor é cópia da mensagem do remetente.

Questão: a mensagem do receptor é realmente uma cópia ou a mensagem foi alterada durante o trânsito ?

UM EXERCÍCIO ...

Para descobrir, eles resumem as duas mensagens e as compara.

Se os resumos forem iguais, ambos sabem que as duas versões são correspondentes. Se os resumos não corresponderem, algo saiu errado.

Como se pode saber que o resumo do remetente não foi alterado ?

55

UM EXERCÍCIO ...

Pode-se saber disso porque ele foi encriptado com a chave privada do remetente.

Como se pode saber que ele foi encriptado com a chave privada do remetente ?

Pode-se saber porque a chave pública apropriada o decripta.

56

ALGUMAS OUTRAS VERIFICAÇÕES ...

Um assinante encriptará um bloco de dados, consistindo de um enchimento, o identificador do algoritmo de resumo e o resumo. O valor encriptado é a assinatura.

O identificador do algoritmo evita que um invasor substitua esse algoritmo, por outro algoritmo de resumo alternativo.

57

ALGUMAS OUTRAS VERIFICAÇÕES ...

Ao usar a chave pública apropriada, essa assinatura é decriptada com o valor do enchimento.

Neste caso, não apenas o resumo, mas o identificador de algoritmo de resumo SHA-X e também os bytes de enchimento são verificados.

58

A CRIPTOGRAFIA BENEFICIA ...

A criptografia de chave simétrica fornece privacidade sobre os dados sigilosos.

A criptografia de chave pública resolve o problema da distribuição de chaves.

Resumo de mensagem - assegura integridade.

59

A CRIPTOGRAFIA BENEFICIA ...

Uma assinatura oferece autenticação.
A entidade que envia dados deve revelar ser a entidade que afirma ser. Os dados são verificados para garantir que vieram dessa entidade.

Uma assinatura também fornece não-repúdio: quem assina não pode mais tarde desautorizar qualquer conhecimento sobre a mensagem.

60

ALGUMAS CONSIDERAÇÕES

Criptografia é uma ciência antiga, mas ainda muito utilizada e importante

- Garante confidencialidade, integridade e autenticação

O segredo está na chave e não no algoritmo

Aumento do poder computacional pode ser um grande problema!!

- Bons criptosistemas são projetados para ser inquebráveis mesmo com a evolução do poder computacional

61

ALGUMAS CONSIDERAÇÕES

Um gerenciamento adequado das chaves é um fator muito importante que não deve ser negligenciado

A criticidade da informação e o tempo que esta deve permanecer confidencial têm muita influência no tamanho da chave

62

BIBLIOGRAFIA

http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/hist.htm

http://pt.wikipedia.org/wiki/Criptoanalise

Anderson, R. *Security Engineering – A Guide to Building Dependable Distributed Systems*. Wiley, 2ª Ed., 2008.

Ferguson, N., Schneier, B. *Practical Cryptography*. Wiley. 2003.

Kurose & Ross, Redes de Computadores e a Internet: uma abordagem top-down. Addison-Wesley. 5ª ed., 2010.

63

BIBLIOGRAFIA

Schneier, B. *Secrets and Lies – Digital Security in a Networked World*. Wiley Publishing, 2003.

Schneier, B. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. Wiley. 1996.

64