Criptografia Simétrica

Sumário:

- Introdução;
- Criptografia simétrica;
- Algoritmos de Criptografia simétrica.

Introdução

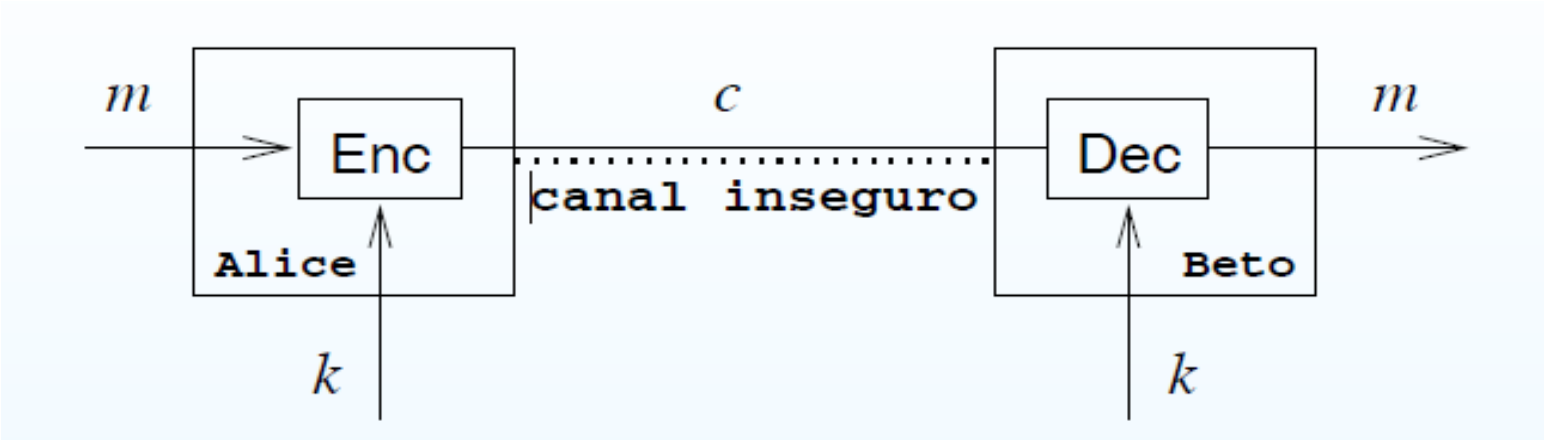
Seja o seguinte Modelo de segurança:

- Entidades: Alice, Beto e o intruso Ivo.
- Os métodos de Ivo podem ser ataque passivo ou até activo (modificação, repetição e injecção de mensagens com objetivos variados como, por exemplo, passar-se por Alice ou Beto para obter acesso a serviços não autorizados)

Introdução

Seja o seguinte Modelo de segurança:

- As técnicas criptográficas para prevenir tais ataques vêm de duas vertentes, a simétrica e a assimétrica, usadas isoladamente ou em conjunto.



Criptografia simétrica

- Alice e Beto desejam trocar mensagens m (*texto claro)* em sigilo (confidencialidade);
- Alice aplica uma *funcão (ou algoritmo) de encriptacão* ENCk(m), que transforma m numa *mensagem encriptada ou texto encriptado c, sob a acção da chave k.*
- Ao receber c, Beto aplica a função de *decriptação* DECk(c), recuperando m.

Criptografia simétrica

- **O objetivo é produzir um texto c que não guarde relação alguma com m.**
- A inclusão da chave k no processo tem o objetivo de dar o poder de transformar c em m apenas a quem conhece k; isto é, prover confidencialidade na transmissão de m.

Criptografia simétrica

- **Por que não criar um algoritmo que não necessite de uma chave?**
  1. As chaves aliviam-nos da necessidade de se preocupar em guardar um algoritmo;
  2. é mais fácil proteger uma chave do que guardar um algoritmo em segredo;
  3. poderá utilizar diferentes chaves para proteger diferentes segredos;

Criptografia simétrica

- **Por que não criar um algoritmo que não necessite de uma chave ?**
  4. Se alguém quebrar uma das suas chaves, os outros segredos ainda estarão seguros;
  5. Se você depender de um algoritmo, um invasor que quebre esse algoritmo, terá acesso a todos os seus dados sigilosos.

Criptografia simétrica - exemplo

- Um exemplo simples de encriptação simétrica consiste em substituir cada letra de um texto pela letra k posições à frente no alfabeto (supomos que após ’z’ vem ’a’).
- Para k = 5, a palavra alabastro se transforma em fqfgfxywt.
- A chave, neste caso é k. Esse é o chamado *método da substituição monoalfabética.*

Criptografia simétrica - exemplo

- Em vez de uma só letra substituindo outra, podemos ter uma lista de letras usadas em sequência. Essa é a *substituição polialfabética.*
- ENC.(.) deve ser projetada de forma que seja muito difícil para Ivo calcular m a partir de c sem conhecimento de k, ainda que ENC.(.) seja pública e Ivo use computadores.

Criptografia simétrica - premissas

- Dizemos que ENCk(.) deve ser uma função *unidirecional para cada valor fixo de k; isto é, que* ENCk(.) seja fácil de calcular, mas ENCk(.) $^{-1}$, ou seja,DECk(.), seja muito difícil de calcular sem o conhecimento da chave k.
- A quantidade de chaves possíveis deve ser muito grande, para evitar uma *busca exaustiva de k.*
- Alice e Beto têm que estabelecer a chave k em sigilo antes do seu uso. Essa dificuldade é recorrente.

Criptografia simétrica - ataques

- Se Ivo conhece a mensagem m na busca exaustiva, o ataque ao modelo é chamado de *ataque do texto claro conhecido.*
- Se somente c fosse conhecido, o ataque seria de *texto encriptado somente.*
- Se Ivo tiver acesso à função ENCk(.), por exemplo embutida em algum dispositivo, e puder produzir pares (m′, c′) à sua escolha, o ataque é de *texto claro escolhido.*

Criptografia simétrica - ataques

- Finalmente, se Ivo tiver acesso à funcão DECk(.) e puder produzir pares (m′, c′) sua escolha, o ataque é de *texto encriptado escolhido.*
- A ciência que se dedica a analisar algoritmos criptográficos em busca de falhas, ou de ”quebrar” tais algoritmos, é a **Criptoanálise.**

Criptografia simétrica - simetria

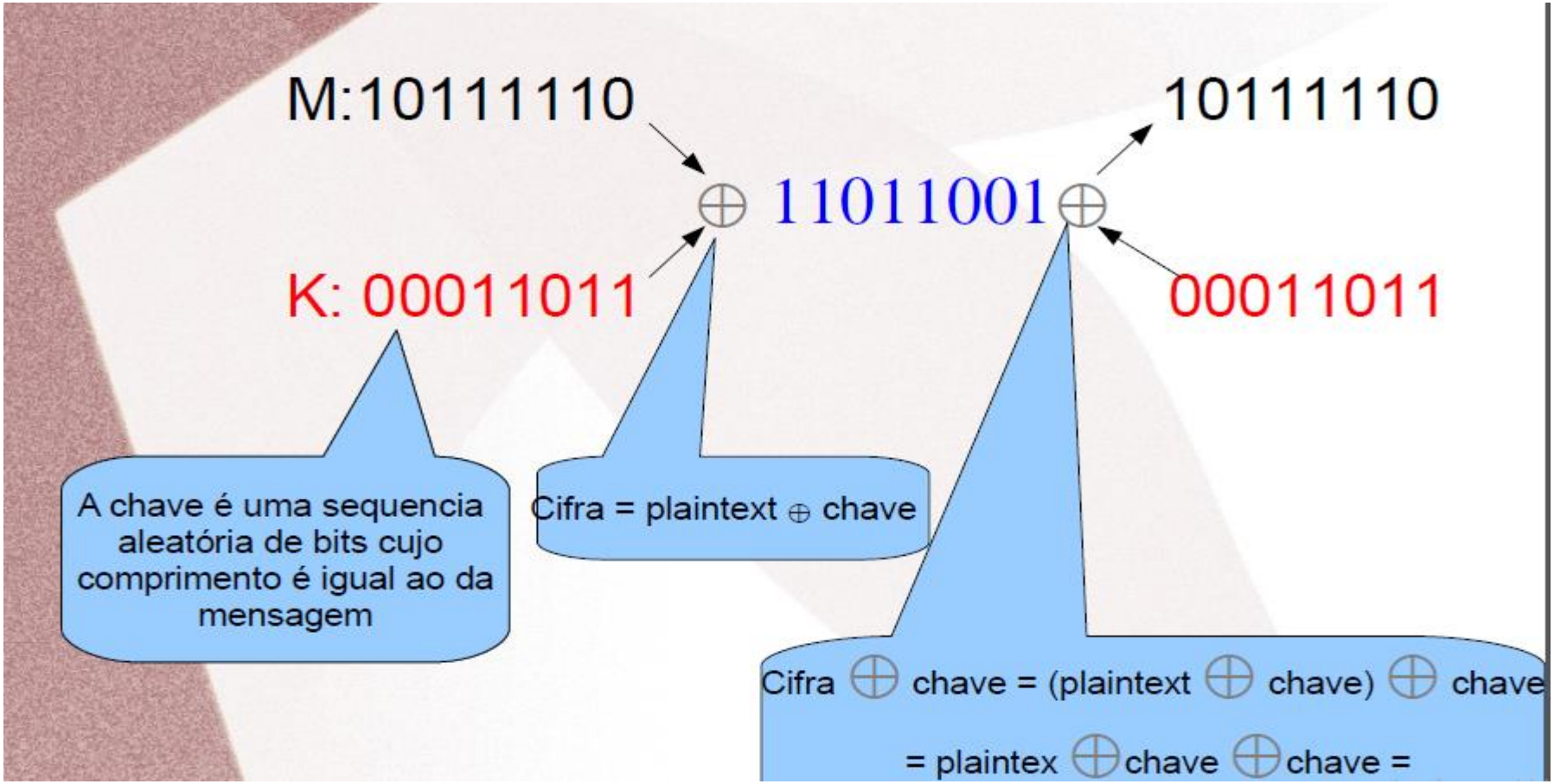
- O adjetivo simétrico é bastante adequado: tudo que um puder encriptar ou decriptar o outro também pode.
- Um benefício dessa simetria é a confiança que Alice e Beto têm de que estão trocando mensagens sigilosas um com o outro, e não com Ivo. Por outro lado, não é possível atribuir a um ou a outro a autoria de uma mensagem sem a ajuda de uma terceira parte confiável.

Criptografia simétrica - simetria

- Outras denominações dos sistemas simétricos são *sistemas de chaves secretas e sistemas de chaves simétricas.*
- **Alguns algorítimos simétricos:**
  - Data Encryption Standard (DES), 1977.
  - Advanced Encryption Standard (AES), 2000.
  - NIST (1997-1999): MARS, RC6, Serpent, Twofish.
  - NESSIE (2003): MYSTY1, AES, Camellia (ISO 2005).

One-time pad

One-Time Pad



One-Time Pad

Vantagens:

- Fácil de computar;
- Teoricamente é seguro:
  - – Dada uma cifra, todos os textos-claro são similares independentemente dos recurso de computação que o atacante possui;
  - – A cifragem atinge a privacidade perfeita só e somente se existe maior número de chaves tanto quanto os textos-claro possíveis e que cada chave só seja igual a si mesmo
    - Desde que a sequência das chaves é aleatória

One-Time Pad

Desvantagens:

- Uma verdadeira aleatoriedade é cara de obter em grande quantidade;
- Inseguro quando as chaves são reusadas;
- A chave deve ter o mesmo comprimento que a mensagem original:
  - Impráctico em muitos senários realísticos;
  - Usado ainda para tráfego em serviços de inteligência e diplomáticos;

One-Time Pad

Desvantagens:

- Não garante integridade:
  - One-time pad garante apenas a confidencialidade;
  - O atacante não pode reconstruir a mensagem original, mas poderá facilmente modifica-la para qualquer coisa;
- Inseguro quando as chaves são reusadas:
  - O Atacante pode obter XOR de plaintexts

Exercícios

- Dadas as chaves seguintes:
  - K1 = 100111010101011
  - K2 = 1011000110
  - K3 = 0001111010101
  - K4 = 1111100
- Encontrar as cifras de:
- M1 = 1990; M2 = 1000011;
- M3 = 1111110001; M4 = 111100011001 1; M5 = 2012;
- M6 = 111111000111010

Criptografia assimétrica e Assinantura digital

Sumário:

- Criptografia assimétrica;
- Algoritmos de Criptografia assimétrica.

Criptografia assimétrica

- Modelo de criptografia criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - na qual **cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública**

Criptografia assimétrica

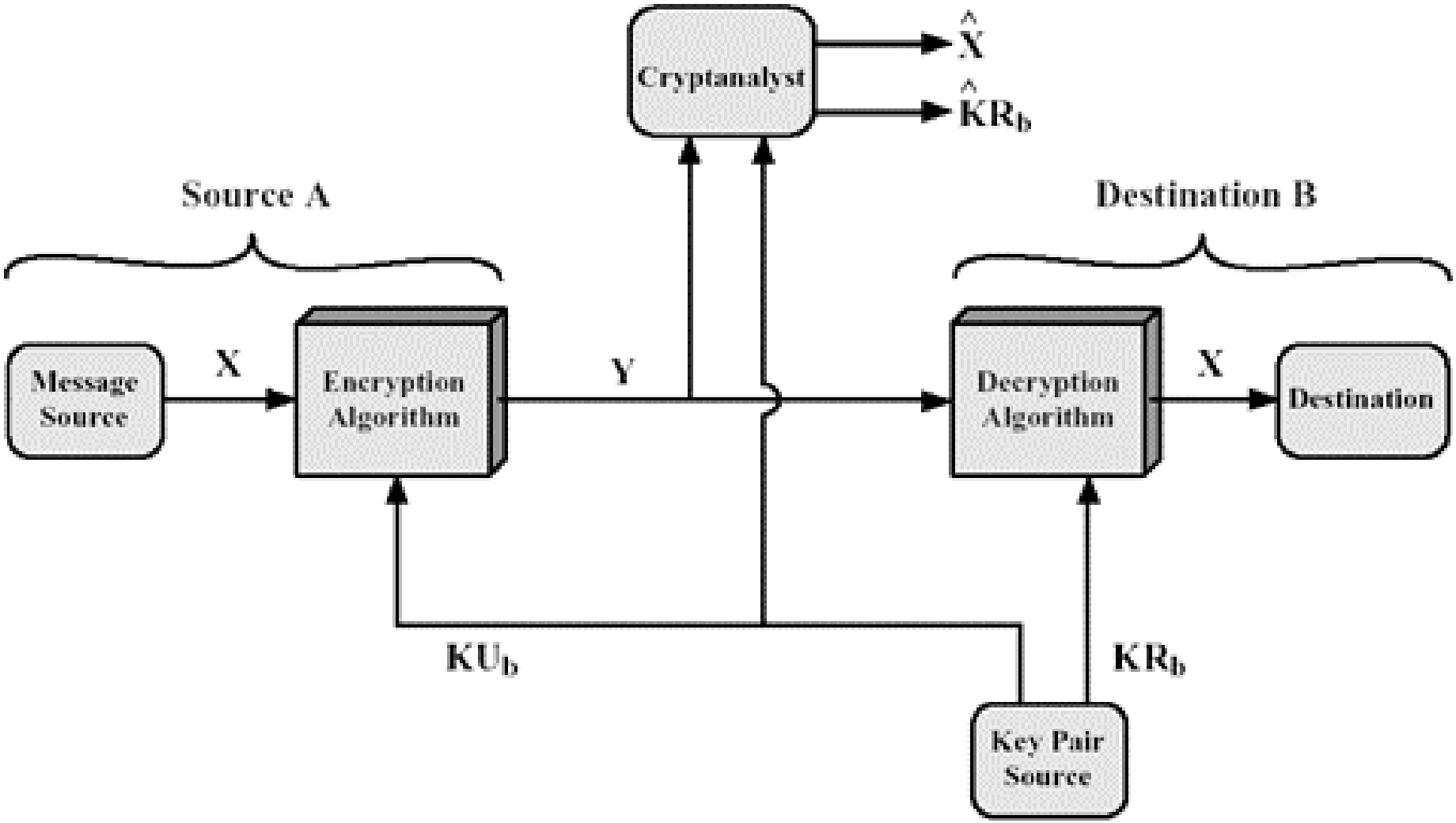
- A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular;
- É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública.

Criptografia assimétrica

- A finalidade de cada chave pode variar em função do que se pretende com o algoritmo assimétrico:

	Finalidade	Chave Pública	Chave Privada
1º	Encriptação de dados	Cifra	Decifra
2º	Assinatura digital	Decifra	Cifra
3º	Encriptação e assinatura digital	Decifra	Cifra
		Cifra	Decifra

Criptografia assimétrica - encriptação



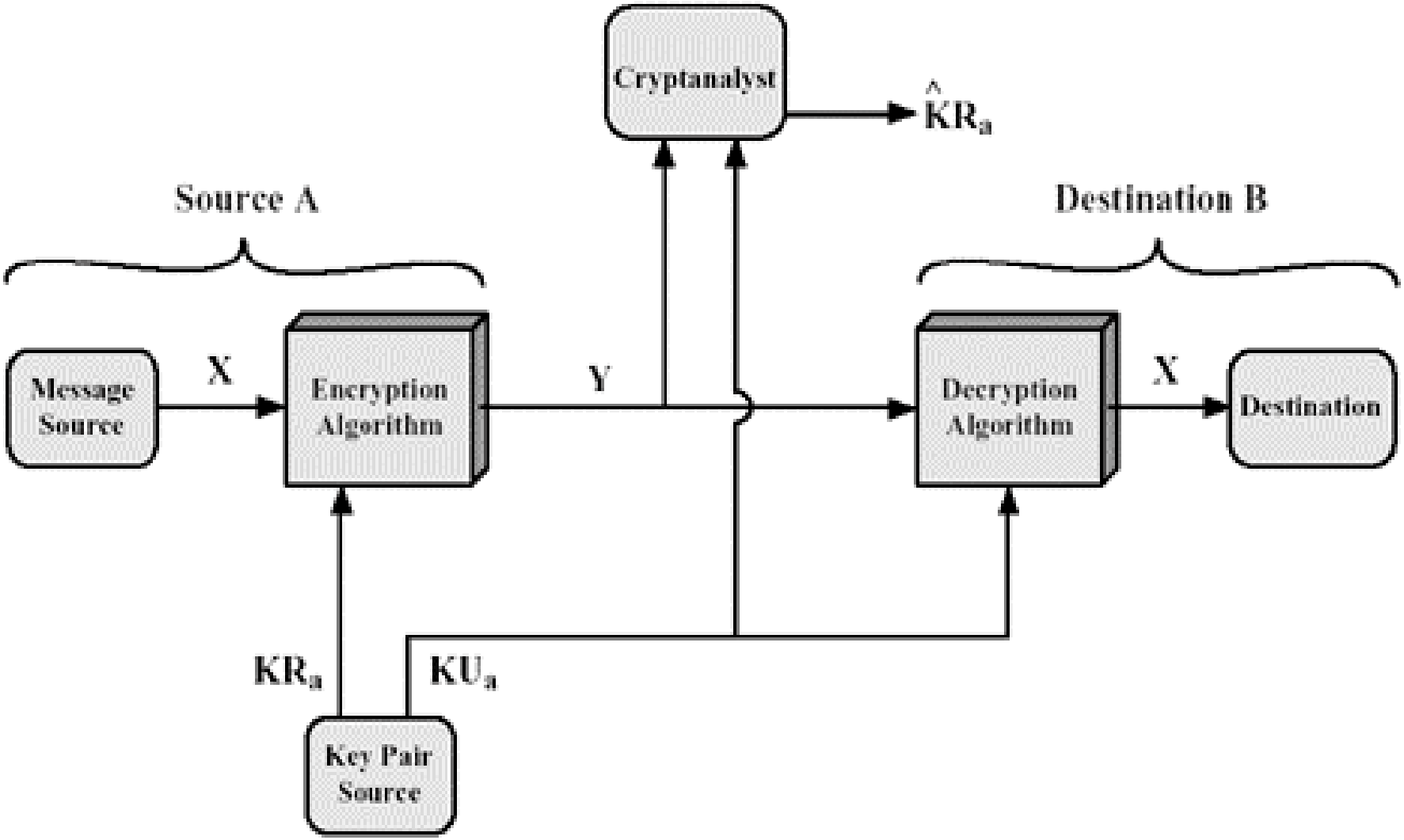
Criptografia assimétrica - encriptação

- Neste caso, vamos exemplificar que Alice quer enviar uma mensagem para Bob, mas somente Bob poderá lê-la.
- Alice irá até Bob através de um canal inseguro qualquer e requisitará a chave pública de Bob.
- Alice irá pegar a mensagem “M” e aplicar a chave pública (KUp) de Bob usando um algoritmo conhecido de todos.

Criptografia assimétrica - encriptação

- Somente Bob tem a chave privada para decifrar a mensagem “C” (Mensagem C é o resultado da mensagem M após aplicar KUp).
- Para tanto, Bob pega o algoritmo conhecido e aplica a sua chave privada (KRb) para obter a mensagem “M” novamente.
- Neste caso a chave pública faz o ciframento e a chave privada faz o deciframento.

Criptografia assimétrica – ass. digital



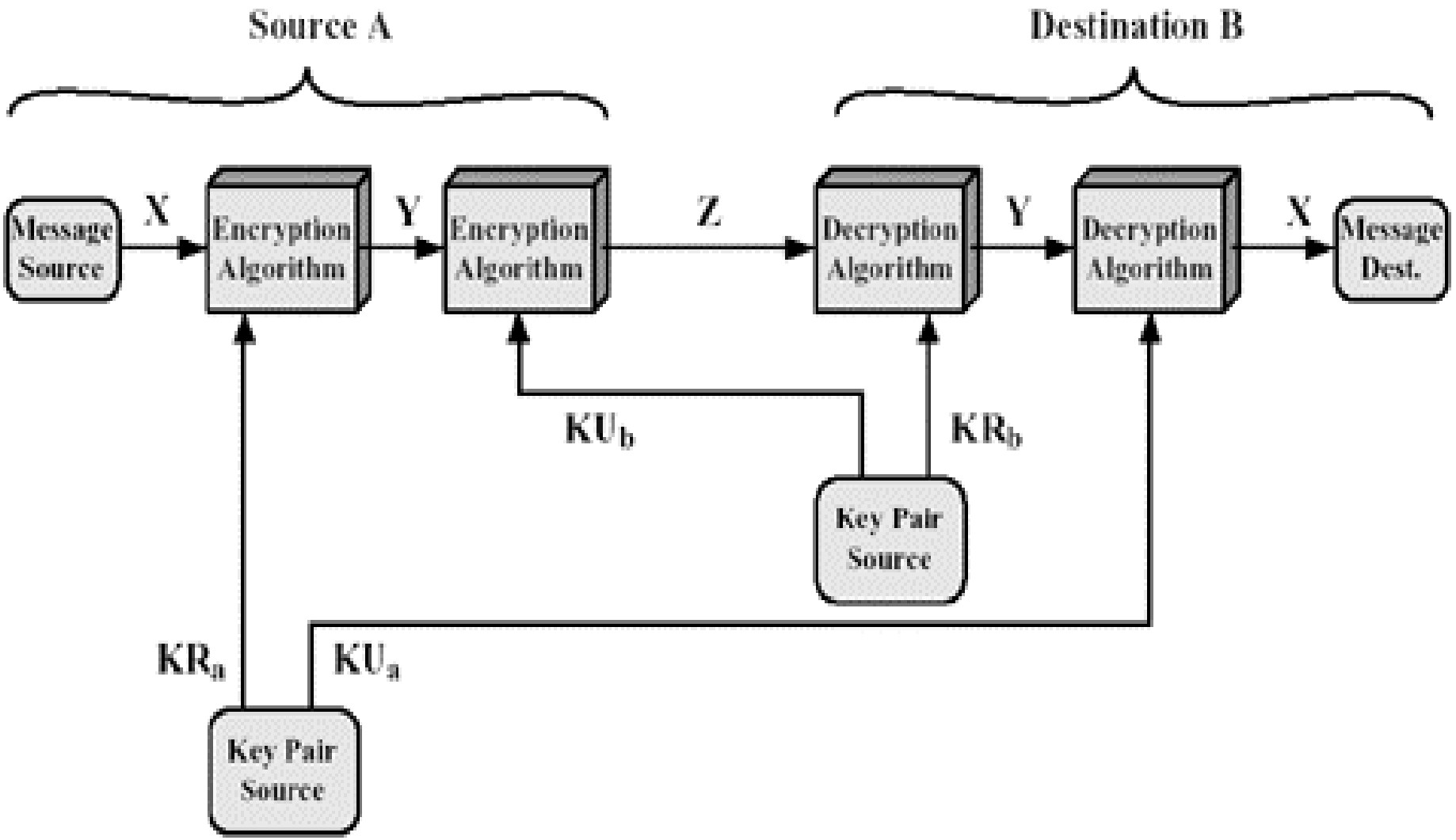
Criptografia assimétrica – ass. digital

- Neste caso, vamos exemplificar que Bob pegará uma mensagem “M” (não cifrada, como por exemplo “vou pagar 1000 reais para Alice”) e aplica a sua chave privada (KRb).
- A chave privada irá fazer a criptografia, ou seja, gerar a mensagem “C”.
- Sendo a chave pública de Bob (KUb) conhecida de todos, qualquer um poderá decriptografar a mensagem.

Criptografia assimétrica – ass. digital

- Se a chave pública de Bob foi capaz de gerar novamente a mensagem “M”, ele e somente ele (Bob) poderia ter gerado a mensagem, garantindo a autoria e autenticação do autor.
- Quando se distribui a mensagem deste jeito, não se garante a confidencialidade dos dados já que a chave KUb é pública e qualquer um poderá ler isto.
- Isto é chamado de assinatura digital.

Encriptação de dados e ass. digital



Encriptação de dados e ass. digital

- Usam-se dois pares de chaves públicas e privadas
- Distribui-se uma chave para criptografar (sigilo) e uma para decriptografar (assinatura digital).
- Deve-se assinar primeiro e cifrar depois, pois assim poderemos verificar a assinatura sem sabermos o conteúdo

Algoritmo RSA (Rivest, Shamir e Adleman)

- Criado em 1977 por Ronald Rivest, Adi Shamir e Len Adleman nos USA;
- É basicamente o resultado de dois cálculos matemáticos. Um para cifrar e outro para decifrar.
- O RSA usa duas chaves criptográficas, uma chave pública e uma privada.
- No caso da criptografia assimétrica tradicional, a chave pública é usada para criptografar a mensagem e a chave privada é usada para decriptografar a mensagem.

Algoritmo RSA

- A sua segurança baseia na dificuldade da factoração de números inteiros extensos;
- Em 1977, os criadores do RSA (Rivest, Shamir e Addleman) achavam que uma chave de 200 bits requereriam 1015 anos, porém chaves com 155 bits foram atacadas em menos de 8 meses;
- Em 2008, chaves com 1024 bits foram quebradas em apenas 100 horas (https://pplware.sapo.pt/informacao/rsa-de-1024-bits-quebrado/);

Algoritmo RSA

- Em níveis críticos, chaves com 2000 bits começam a ser usadas.
- Para tanto vale lembrar que “M” é a mensagem que queremos cifrar (plaintext), “C” é a mensagem cifrada, “e” é a chave pública, “d” é a chave privada
- e “n” é um número que é calculado e que todos sabem (público).

Algoritmo RSA

1. Criptografar: $C = M^e \bmod n$
2. Decriptografar: $M = C^d \bmod n$
3. Para cada bloco a ser cifrado deve -se fazer o cálculo acima. Ambos devem saber o valor de “n”. Portanto, a chave pública definida pela dupla “e” e “n”, sendo KUa = {e, n}. A chave privada é definida pela dupla “d” e “n”, sendo KRb = {d, n}.

Algoritmo RSA

Passos para a geração da chave:

1. Seleccionar dois números primos *p* e *q* grandes (geralmente maior que 10^{100}).
2. Calcule o valor de n = p . q
3. Calcule *fn* = (*p* -1) × (*q* -1)
4. Selecione um inteiro “d” relativamente primo à *fn*
5. Calculamos “e” de forma que (e . d) mod *fn* = 1

Algoritmo RSA

Exemplo:

1. p = 3 e q = 11

2. n = 3 * 11, logo n = 33

3. *fn* = (3 -1) × (11 -1) = 2 ×10 , portanto *fn* =20

4. d é um inteiro relativamente primo à *fn* , e atende 1 < d < *fn*

d = 7

(11, 13, 17 e 19 seriam outras opções)

(não seria possível 5 já que 5 vezes 4 = *fn* (20))

5. Calculamos “e” de forma que (e . 7) mod 20 = 1

e = 1 => (1.7) = 7 mod 20 ¹ 1 => falso

e = 2 => (2.7) = 14 mod 20 ¹ 1 => falso

e = 3 => (3.7) = 21 mod 20 = 1 => verdadeiro

(outros múltiplos de 3 seriam possíveis (6,9,12, etc)).

Algoritmo RSA

Portanto teríamos KU = {3, 33} e KR = {7, 33}. Lembrando que neste caso *e*, *d* e *n* tem menos de 2^6, então temos apenas 6 bits.

Se tivéssemos um texto com o número 20, uma mensagem cifrada seria:

$C = M^e \bmod n$

$C = 20^3 \bmod 33$

$C = 8000 \bmod 33$

$C = 14$

E para decifrar:

$M = C^d \bmod n$

$M = 14^7 \bmod 33$

$M = 105.413.504 \bmod 33$ (resposta = 3.194.348 x 33 + 20 = 105.413.504)

$M = 20$

Criptografia simétrica vs assimétrica

	Criptografia Simétrica	Criptografia Assimétrica
Funcionamento	O mesmo algoritmo é usado para criptografar e decriptografar a mensagem	O mesmo algoritmo é usado para criptografar e decriptografar a mensagem, porém usando duas chaves.
Requer	Que destino e origem saibam o algoritmo e a chave	A origem e o destino devem saber uma (somente uma) chave do par de chaves. Todos podem ter a chave pública, porém só 1 deve saber a chave privada.
Segurança	A chave deve ser mantida em segredo	Apenas 1 das duas chaves deve ser mantida em segredo
	Mesmo sabendo o algoritmo e tendo exemplos dos textos criptografados **deve** impossibilitar a determinação da chave.	É impossível decifrar uma mensagem mesmo tendo acesso ao algoritmo, à chave pública e a exemplos dos textos cifrados.

Criptografia simétrica vs assimétrica

	Criptografia Simétrica	Criptografia Assimétrica
Utilidade	Privacidade	Tendo a chave pública deve ser impossível chegar na chave privada. • Identificação • Assinatura Digital • Privacidade • Troca de Chaves • (muitas utilidades)
Velocidade de Processamento	Muito Rápida	Lenta
Chaves	Apenas uma	2 Chaves (Pública e Privada)

Obrigado!

Assinatura digital e Autoridades de Certificação

Sumário:

- Assinatura digital;
- Autoridades de certificação (AC)

Assinatura digital

- Pelas razões explicadas anteriormente, **o uso de algoritmos assimétricos tende a ser restrito à proteção de chaves simétricas e para a oferta de assinaturas digitais**.
- Se existe uma necessidade de resolver disputas entre emissor e receptor tal como para os conteúdos de uma mensagem ou da sua origem, em seguida, a utilização de criptografia simétrica não fornece a resposta.
- As assinaturas digitais são obrigatórios.

Assinatura digital

- A **assinatura digital** de uma mensagem de um remetente particular, é um valor criptográfico que **depende da mensagem e do remetente**.
- Em contraste, uma assinatura manuscrita depende apenas do remetente, e é a mesma para todas as mensagens.
- Uma assinatura digital fornece a integridade dos dados e prova de origem (não-repúdio).

Assinatura digital

- Para um esquema de assinatura digital com base em um sistema de chave pública, como RSA ou El Gamal, o princípio básico é muito simples.
- Cada usuário tem uma chave privada que somente ele podem usar, e seu uso é aceite para identificá-lo. Para além disso, existe uma chave pública correspondente que qualquer um que conhece e pode verificar se a chave privada correspondente foi usado, mas não pode determinar a chave privada.

Assinatura digital

- Aceitando-se que a chave privada foi usado dá ao receptor a garantia quer da origem quer do conteúdo da mensagem.
- Portanto, o remetente é re-assegurado de que a representação é impossível uma vez que a chave privada (ou assinatura) não pode ser deduzida a partir da chave pública (ou de verificação) ou da assinatura digital.

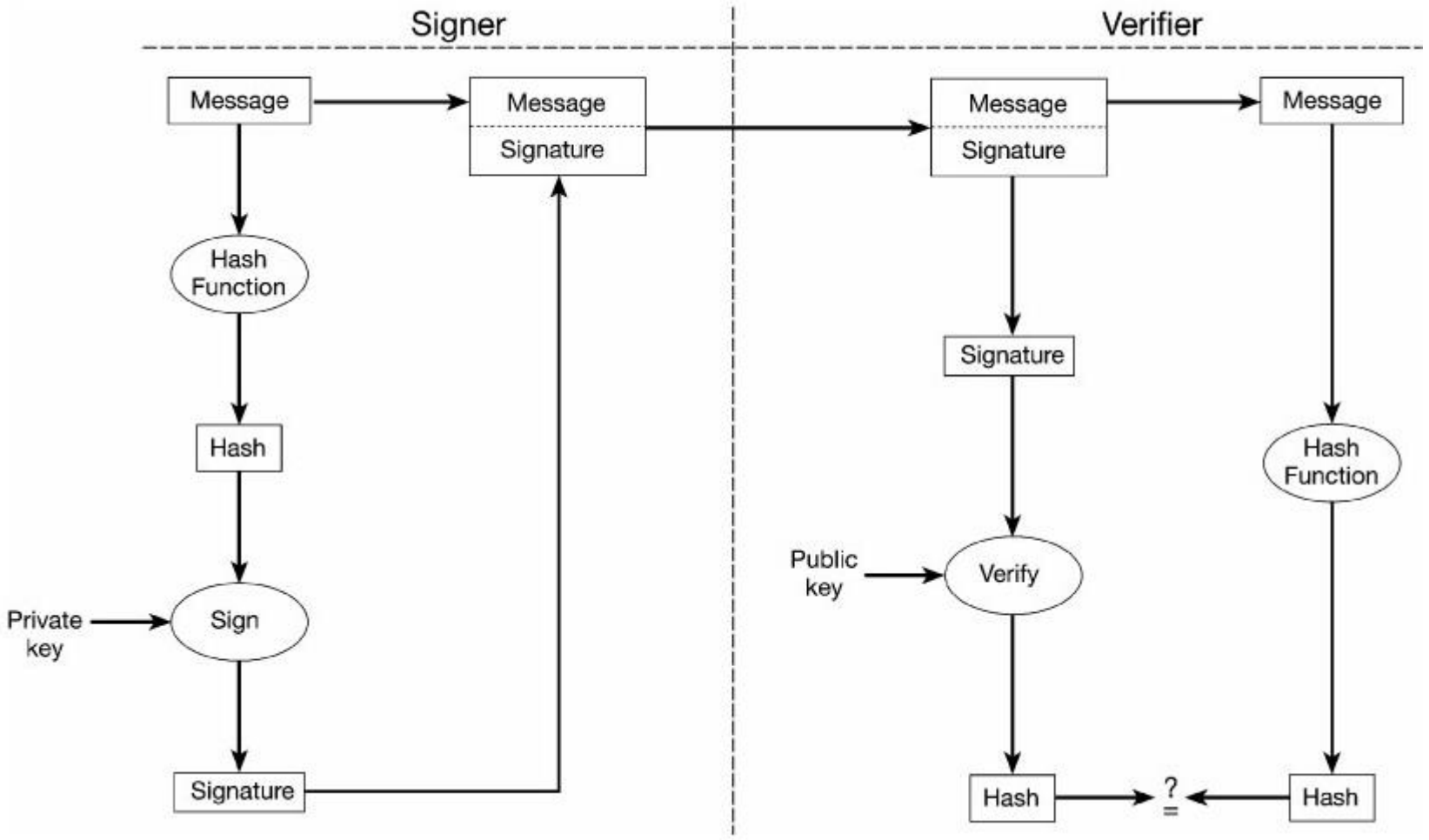
Assinatura digital

- O processamento criptográfico assimétrico exige muito processamento computacional.
- Assim, uma versão compacta ou hash da mensagem é produzida por aplicação de uma função hash para a mensagem.
- A assinatura é produzida a partir do hash (que representa a mensagem) usando o algoritmo assimétrico com a chave privada.
- Assim, apenas o proprietário da chave privada pode gerar a assinatura.

Assinatura digital

- A assinatura pode ser verificada por qualquer pessoa que conheça a chave pública correspondente.
- Para fazer isso, um valor é produzido a partir da assinatura utilizando o algoritmo assimétrico com a chave pública.
- Este valor deve ser o hash da mensagem, que qualquer pessoa pode calcular. Se este valor e o hash corresponderem, a assinatura é aceite como verdadeira. Se eles discordarem, a assinatura não é genuína.

Assinatura digital



Assinatura digital

- Os dois algoritmos assimétricos mais utilizados são RSA e El Gamal.
- Para o RSA, a criptografia e descriptografia são idênticos, de modo que os processos de assinatura e verificação também são idênticos.
- Uma alternativa a RSA é o Digital Signature Standard (DSS), que se baseia em El Gamal

Ataques de Personificação

- Suponha que assinaturas digitais estão a ser utilizados como um método de identificação. Se o usuário "**A**" deseja representar o usuário "**B**", então existem duas formas diferentes de ataque:

1. "**A**" tenta quebrar a chave privada do "**B**"; ou
2. "**A**" tenta substituir sua chave pública para a chave pública de "**B**".

Ataques de Personificação

- Ataques do primeiro tipo envolvem ou tentando quebrar o algoritmo ou ter acesso aos dispositivos físicos que armazenam a chave privada;
- TPC:
  - Ataques contra o algoritmo
  - Segurança física para a gestão de chaves

Ataques de Personificação

- Suponha que o usuário **“A”** foi capaz de estabelecer sua chave pública como pertencente a usuário B.
- Outros usuários usariam então a chave pública de **“A”** para criptografar chaves simétricas para “**B”**. No entanto **“A”**, ao contrário de “**B”**, obteria a informação secreta protegida por essas chaves simétricas.

Ataques de Personificação

- Além disso, **“A”** seria capaz de assinar as mensagens usando a sua chave privada, e estas assinaturas seriam aceites como sendo de “**B**”.
- O uso de Autoridades de Certificação e o estabelecimento de infra-estruturas de chave pública (PKI) destinam-se a impedir que esses ataques de personificação ocorram.

Autoridades de Certificação

- O principal papel de uma Autoridade de Certificação (AC) é fornecer certificados assinados digitalmente que “ligam” a identidade de uma entidade ao valor da sua chave pública.
- A fim de que os certificados da AC possam ser verificados, a própria chave pública do AC deve ser amplamente conhecida e aceite.

Autoridades de Certificação

- Neste contexto, um certificado é uma mensagem assinada que contém a **identidade** da entidade, o valor de sua **chave pública**, e provavelmente alguma **informação extra**, tal como uma data de expiração.
- Estes certificados podem ser pensados como uma 'carta de apresentação' a partir de uma fonte respeitada (AC).

Autoridades de Certificação

- Suponha que CERTA é um certificado emitido pela AC que contém a identidade de A e chave pública de A, assim, CERTA “liga” a identidade de A ao seu valor de chave pública.
- Qualquer pessoa com uma cópia autêntica da chave pública do AC pode verificar se a assinatura no CERTA está correta e, assim, obter a garantia de que eles sabem a chave pública de A.

Autoridades de Certificação

- Assim, o problema de garantir a autenticidade da chave pública de A foi substituído pela necessidade de ser capaz de garantir a autenticidade da chave pública da AC, juntamente com a confiança de que a verificação da identidade de A foi realizada correctamente.
- Note que qualquer pessoa que pode representar A durante o processo de certificação pode obter um certificado que “liga” sua chave pública à identidade de A.

Autoridades de Certificação

- Isto permite-lhes representar A durante toda a vida útil do certificado.
- Este é um exemplo do problema potencialmente preocupante de roubo de identidade que é susceptível de aumentar no futuro.

Autoridades de Certificação

- É importante notar que qualquer pessoa pode ser capaz de produzir um determinado certificado do usuário para que a propriedade do certificado digital do usuário A não identifica A.
- O certificado apenas liga a identidade de A para um valor de chave pública.
- A prova de identidade pode então ser estabelecida pela utilização de um protocolo de desafio-resposta que prova a utilização da chave privada de A.

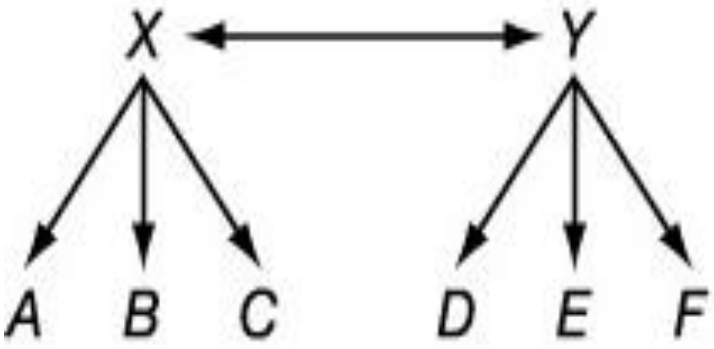
Autoridades de Certificação

- Isso pode envolver que A seja emitido com um desafio para assinar.
- A retorna-o com a sua assinatura e o verificador confirma a validade da assinatura utilizando o valor de chave pública no certificado de A.
- É a utilização da chave privada correspondente à chave pública dada no certificado de A que define a identidade de A.

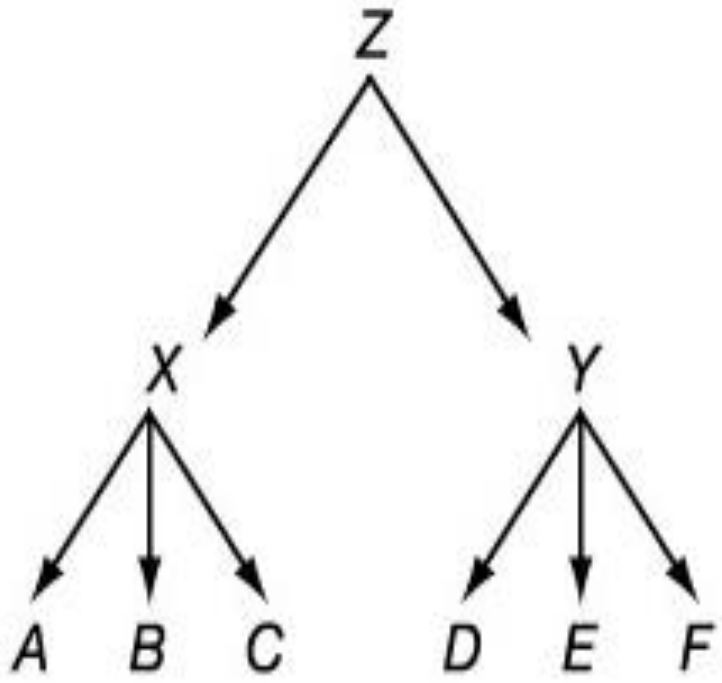
Autoridades de Certificação

- Suponha agora que dois usuários, A e B, têm certificados emitidos por diferentes AC's.
- Se precisa de uma garantia sobre a autenticidade da chave pública de B, então A precisa de uma cópia autêntica da chave pública da AC do B.
- Isso pode ser conseguido por certificação cruzada, em que cada uma das duas AC's emite um certificado para o outro, ou a introdução de uma hierarquia de certificação, onde uma AC raiz fica acima dessas duas AC´s e emite certificados para cada um deles.

Autoridades de Certificação



(a)
Cross certification



(b)
A certification hierarchy

Autoridades de Certificação

- Os diagramas ilustram os dois processos.
- Em cada caso, X e Y são AC´s enquanto X → A significa que X emite um certificado para A.
- Em (b), o símbolo Z representa uma AC raiz.
- Se, por exemplo, B precisa de confiança na chave pública de E, então, para o (a) B precisa verificar o certificado para Y emitido pelo X e o certificado para E emitido por Y.

Autoridades de Certificação

- Para (b) B precisa verificar o certificado de Y emitida por Z e os certificados de E emitido por Y.
- Assim, em cada caso, B precisa verificar uma cadeia de dois certificados.
- Para sistemas mais complexos que envolvem uma combinação de muitas cruzadas certificações e hierarquias com mais de um nível, essa cadeia pode ser consideravelmente mais longo.

Problemas com AC´s

- Um dos principais problemas associados com a utilização de certificados é o problema de revogação.
- Por exemplo, uma empresa pode emitir um certificado para um empregado que deixa a empresa mais tarde.
- Um segundo exemplo é o de um keyholder que sabe que a sua chave privada ficou comprometida.

Problemas com AC´s

- Em ambos os casos, existe um requisito para a AC ser capaz de revogar o certificado.
- Uma vez que esses certificados são susceptíveis de ter sido amplamente distribuído, é pouco provável que seja prático notificar todos diretamente.
- Uma solução comum é a AC publicar uma lista de revogação de certificados (CRL). No entanto, esta é uma sobrecarga de gerenciamento significativa e tem muitos problemas associados.

Autoridades de Certificação

- Um segundo problema óbvio refere à responsabilidade.
- Muitos usuários irão confiar em tais certificados.
- Suponha que um certificado está errado, no sentido de que o valor da chave pública listada não pertence ao proprietário listado. Neste caso, pode não ser claro quem é responsável: o proprietário, o utilizador ou o AC.

Obrigado!