Redes de Computadores
RCP 22108

Prof. Samir Bonho

Engenharia Eletrônica

Origens

- Cifra de César:
  - O Imperador Júlio César utilizou em suas correspondências pessoais em 50 a.c.
  - Atualmente denomina-se César toda cifra que consiste em deslocar cada letra da mensagem original, por um número fixo de posições
  - Também tem registro de utilização na Guerra da Secessão americana, e pelo exército Russo na I Guerra Mundial (1915)

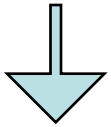
Origens

ABCDEFGHIJKLMNOPQRSTUVWXYZ

altera 5 posições

VWXYZABCDEFGHIJKLMNOPQRSTU

O BOCA MOLE



J WJXV HJGZ

Texto Claro

5 **Chave**

Texto **Cifrado**

Utilização

- Para garantir e reforçar os aspectos de segurança de:
  - Sigilo
  - Integridade
  - Autenticação

Definições

- Cifrar ou Codificar ou Encriptar
  - Ato de transformar dados em alguma forma ilegível
  - Propósito: garantir a privacidade, mantendo a informação incompreensível para pessoas não autorizadas, mesmo que estas tenham acesso aos dados cifrados
- Decifrar ou Decodificar ou Decriptar
  - Processo inverso ao de cifrar, consiste em retornar a informação a sua forma legível

O papel da criptografia

- D**e modo algum a criptografia é a única ferramenta** para assegurar a segurança da informação.

- Nem resolverá todos os problemas de segurança.

- Criptografia **não é a prova de falhas**.

O papel da criptografia

- Toda criptografia pode ser quebrada e , sobretudo, se for **implementada incorretamente**, não agrega nenhuma segurança real.

Definições

- Os procedimentos de criptografar e decriptografar são obtidos através de um algoritmo.

Dois princípios fundamentais da criptografia

- Redundância de informação
- Atualidade de mensagens

Princípio Criptográfico #1

Redundância

- As mensagens criptografadas devem conter alguma redundância
  - Informações não necessárias para compreensão da mensagem clara.
  - Todas as mensagens devem conter informações redundantes suficientes para que os intrusos ativos sejam impedidos de transmitir dados inválidos que possam ser interpretados como uma mensagem válida.

Princípio Criptográfico #2

Atualidade

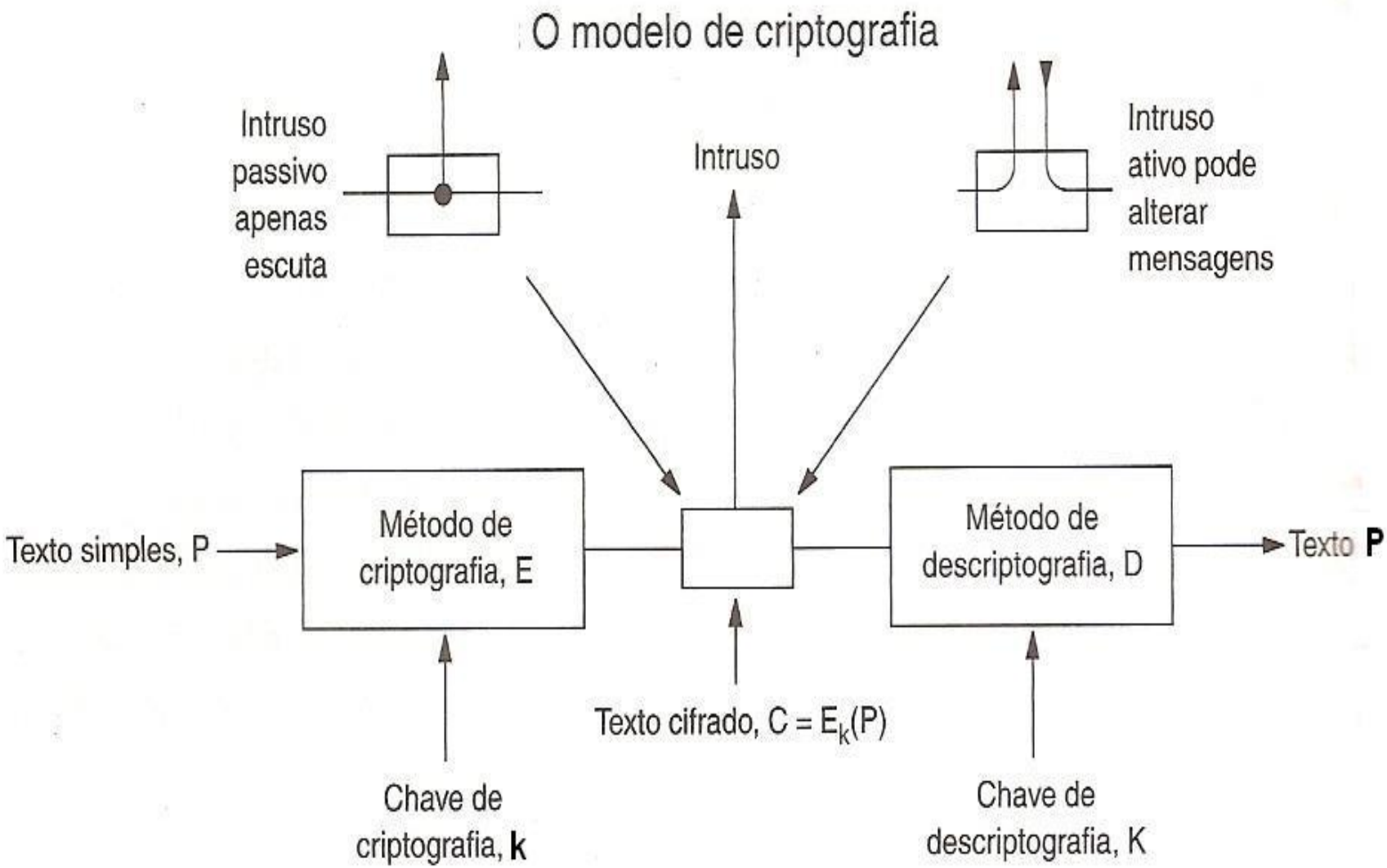
- Algum método é necessário para anular ataques de repetição.
- Medidas para assegurar que cada mensagem recebida possa ser confirmada como uma mensagem atual (enviada muito recentemente).

Princípio Criptográfico #2

Atualidade

- Medida necessária para impedir que intrusos ativos reutilizem (repitam) mensagens antigas por intermédio de interceptação de mensagens no meio de comunicação.

- Timestamp válido por um pequeno período de tempo


O modelo de criptografia
Intruso passivo apenas escuta
Intruso
Intruso ativo pode alterar mensagens
Texto simples, P
Método de criptografia, E
Método de descriptografia, D
Texto P
Texto cifrado, C = E_k(P)
Chave de criptografia, k
Chave de descriptografia, K

Equações da Criptografia

$$D_k (E_k(P)) = P$$

E e D são funções matemáticas

K é uma **chave**

Conceito de Código

- Substitui uma palavra por outra palavra ou uma palavra por um símbolo.

- Códigos, no sentido da criptografia, não são mais utilizados, embora tenham tido uma história …
  - O código na linguagem navajo dos índios americanos, utilizado pelos mesmos contra os japoneses na Segunda Guerra Mundial.

Conceito de Cifra

- É uma transformação de caractere por caractere ou bit pot bit, sem levar em conta a estrutura linguística da mensagem.
  - Substituindo um por outro.
  - Transpondo a ordem dos símbolos.

- Três dimensões para classificar os sistemas criptográficos:
  - Tipo de operações usadas para transformar o texto
    - Substituição – cada elemento é mapeado em outro elemento
    - Transposição – elementos no texto em claro são rearrumados
  - Número de chaves usadas
    - Simétrica (uma única chave)
    - Assimétrica (duas chaves – cifragem de chave pública)
  - A forma na qual o texto em claro é processado
    - *Block cipher* (cifragem de bloco)
    - *Stream cipher* (cifragem de fluxo)

Cifras de Substituição

e

Cifras de Transposição

Cifras de Substituição

- Cada **letra** ou **grupo de letras** é substituído por **outra letra** ou **grupo de letras**, de modo a criar um “disfarce”.

- Exemplo: A Cifra de César (Caeser Cipher). Considerando as 26 letras do alfabeto inglês (a,b,c,d,e,f,g,h,I,j,k,m,n,o,p,q,r,s,t,u,v,x,w,y,z),

  Neste método, ***a*** se torna ***d***, ***b*** se torna ***e***, ***c*** se torna ***f***, … …, ***z*** se torna ***c***.

Generalização da Cifra de César

- Cada letra se desloca *k* vezes, em vez de três. Neste caso, k passa a ser uma chave para o método genérico dos alfabetos deslocados de forma circular.

Cifras de Substituição Monoalfabética

- Próximo aprimoramento:
  - Cada letra do texto simples, do alfabeto de 26 letras, seja mapeada para alguma outra letra.
- a -> Q, b -> W, c -> E, d -> R, e ->T, ...

- Esse sistema geral é chamado **cifra de substituição monoalfabética.**

Cifras de Substituição Monoalfabética

- Sendo a **chave** uma *string* de 26 letras correspondente ao alfabeto completo.

- Quebra da chave: **26!** chaves possíveis.
  - Computador com o tempo de processamento de instrução de 1 ns. Tempo para quebrar a chave de 10^10 anos.

Cifras de Substituição Monoalfabética

- Entretanto, apesar de parecer seguro, com um volume de texto cifrado surpreendentemente pequeno, a cifra pode ser descoberta.

- Estratégia: a propriedades estatísticas dos idiomas.

Cifra de Transposição

- Cifras de Transposição reordenam os símbolos, mas não os disfarçam.
  - Exemplo: cifra de transposição de colunas.

Exemplo de Cifra de Transposição

- A cifra se baseia numa chave que é uma palavra ou uma frase que não contém letras repetidas.
- Seja a chave: MEGABUCK
- O objetivo da chave é numerar as colunas de modo que a coluna 1 fique abaixo da letra da chave mais próxima do início do alfabeto e assim por diante.

Exemplo de Cifra de Transposição

- O texto simples é escrito horizontalmente, em linhas.

- O texto cifrado é lido em colunas, a partir da coluna cuja letra da chave tenha a ordem mais baixa no alfabeto.

- A numeração abaixo da chave, significa a ordem das letras no alfabeto.

Exemplo de Cifra de Transposição

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Exemplo de Cifra de Transposição

- Algumas cifras de transposição aceitam um bloco de tamanho fixo como entrada e produzem um bloco de tamanho fixo como saída.

- Essas cifras podem ser completamente descritas fornecendo-se uma lista que informe a ordem na qual os caracteres devem sair.

Exemplo de Cifra de Transposição

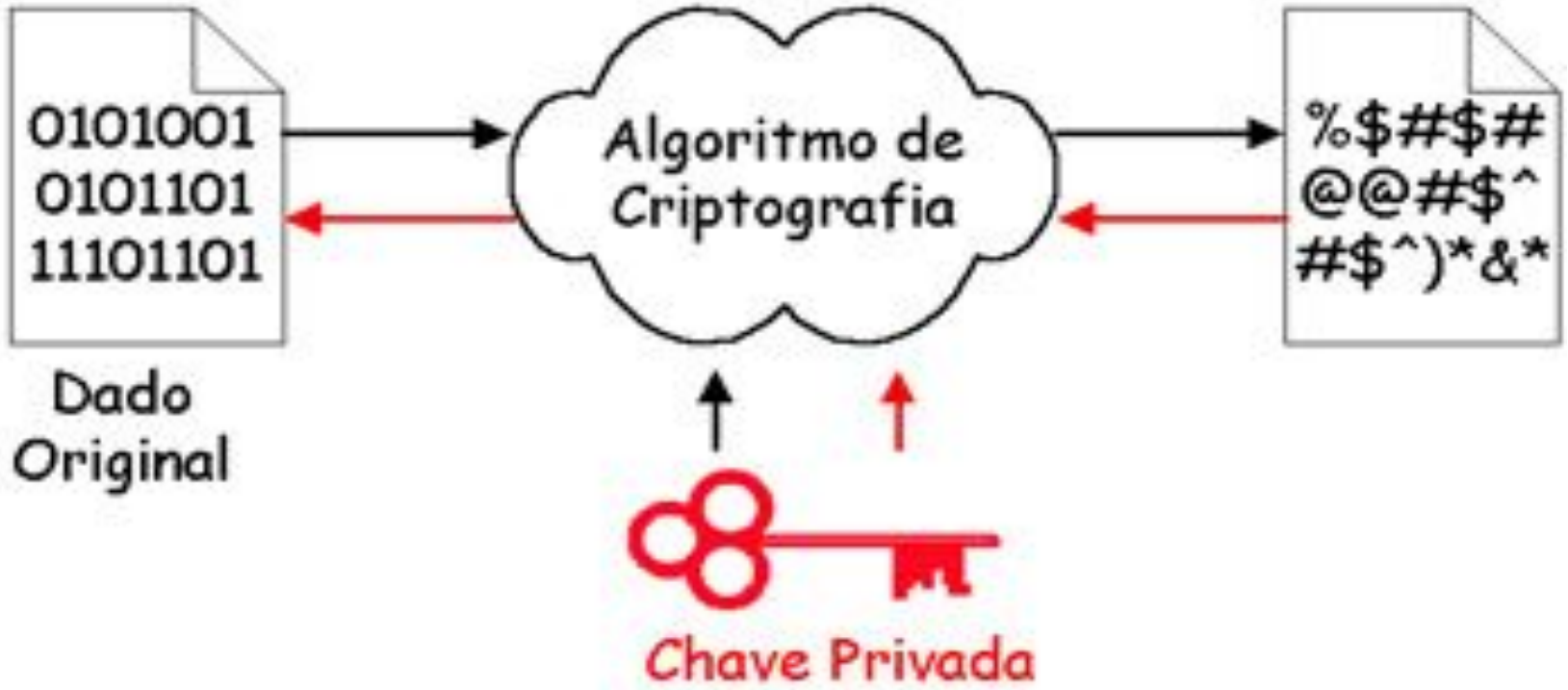
- No exemplo, a cifra pode ser vista como uma **cifra de blocos de 64 bits de entrada**.

- Para a saída, a lista para a ordem de saída dos caracteres é 4, 12, 20, 28, 36, 44, 52,60, 5, 13, ... 62.

- Neste exemplo, o quarto caractere de entrada, ***a***, é o primeiro a sair, seguido pelo décimo segundo, ***f***, e assim por diante.

Criptografia Simétrica

Criptografia Simétrica



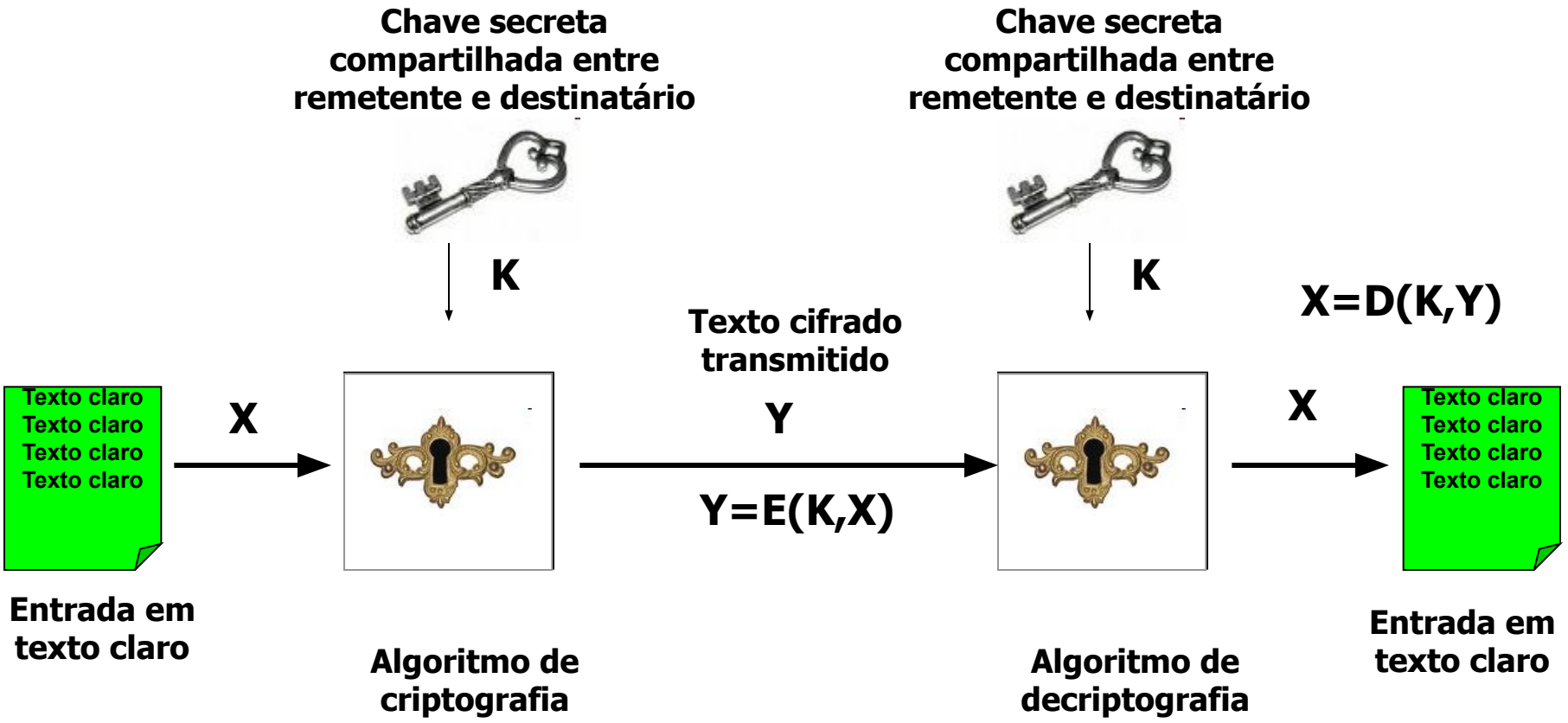
Modelo de criptografia simétrica

- O modelo simétrico de criptografia possui cinco componentes:
  - Texto claro
    - Mensagem ou dados originais em texto claro, inteligíveis
  - Algoritmo de criptografia
    - Conjunto de procedimentos que realizam a transformação no texto claro
  - Chave secreta
    - A chave é um valor independente do texto claro e também serve de entrada para o algoritmo de criptografia
  - Texto cifrado
    - Mensagem embaralhada pelo algoritmo de criptografia
  - Algoritmo de decriptografia
    - Algoritmo de criptografia operado no modo inverso

Modelo de criptografia simétrica

- Requisitos para uso seguro da criptografia simétrica (convencional)
  - Algoritmo de criptografia forte
    - Mesmo o oponente conhecendo o algoritmo e o texto cifrado não seja capaz de decifrá-lo ou descobrir a chave
    - O emissor e o receptor precisam ter cópias seguras da chave criptográfica

Modelo de criptografia simétrica



Criptografia Simétrica: Distribuição de chaves

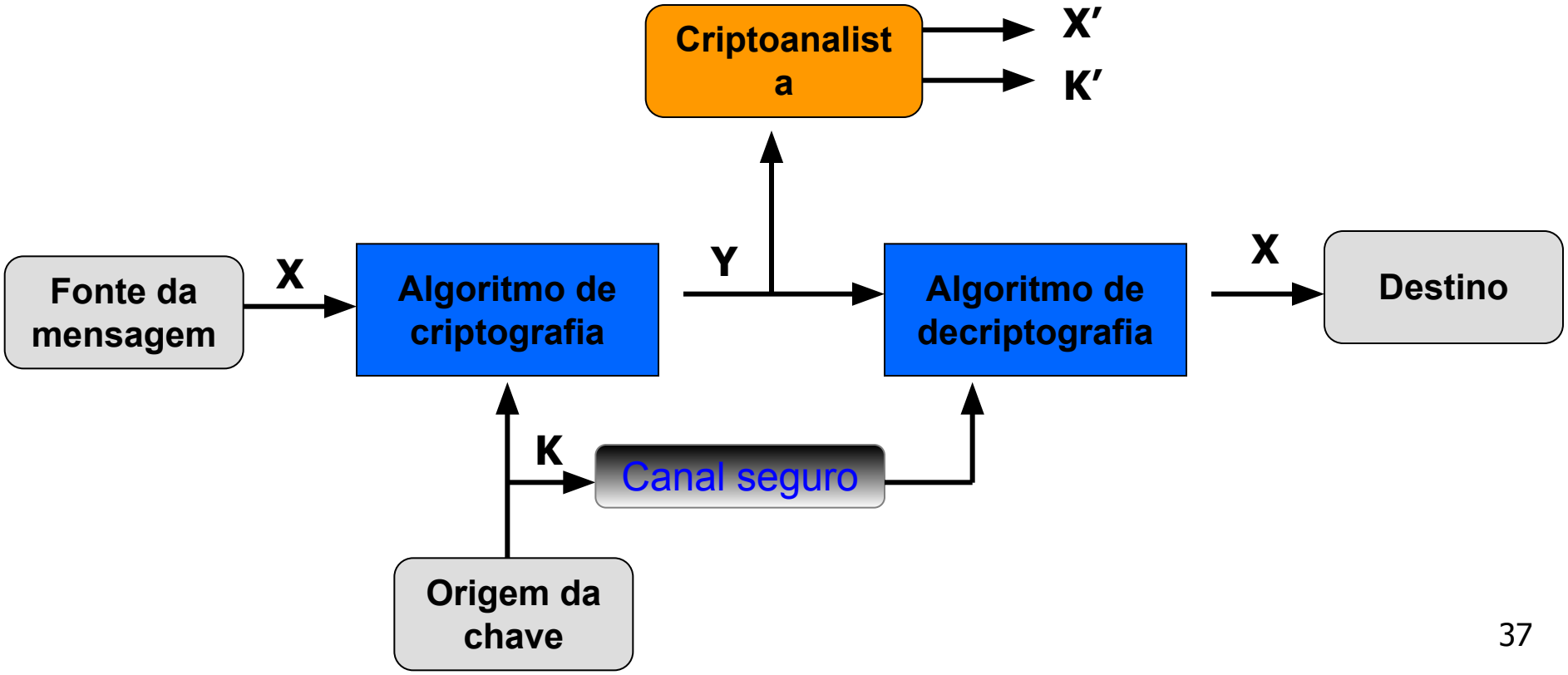
- Para a criptografia simétrica funcione, as duas partes precisam compartilhar a mesma chave
- A chave precisa ser protegida contra acesso de outras partes
- Formas para distribuição das chaves
  - **A** pode selecionar uma chave e entregá-la fisicamente a **B**
  - Um terceiro pode selecionar uma chave e entregar a **A** e **B**
  - **A** e **B** podem trocar novas chaves utilizando chaves anteriormente trocadas
  - Se **A** e **B** tiverem uma comunicação criptografada com um terceiro **C**, C pode entregar seguramente uma chave para **A** e **B**

Modelo de criptografia simétrica

- Todos os algoritmos de criptografia baseiam-se nos métodos de:
  - Substituição
    - Cada elemento do texto claro (bit, letra, grupo de bits, grupo de letras) é mapeado em outro elemento
  - Transposição (Reorganização do texto)
    - Reorganização do texto claro, embaralhamento
- O requisito fundamental é não haver perda de informação no processo de cifragem

Modelo de criptografia simétrica

- Modelo de criptosistema convencional



Modelo de criptografia simétrica

- Principais ataques de criptoanálise

Tipo de ataque	**Conhecido ao criptoanalista**
Apenas texto cifrado	▪Algoritmo de criptografia ▪Texto cifrado
Texto claro conhecido	▪Algoritmo de criptografia ▪Texto cifrado ▪Uma ou mais partes do texto claro / texto cifrado com a chave secreta
Texto claro escolhido	▪Algoritmo de criptografia ▪Texto cifrado ▪Texto claro escolhido pelo criptoanalista juntamente com o texto cifrado correspondente

* Existem variações desses ataques

Modelo de criptografia simétrica

- Esquema de criptografia computacionalmente seguro
  - Quando o custo para quebrar a cifra for superior ao valor da informação codificada
  - Tempo exigido para quebrar a cifra superior ao tempo de vida útil da informação

Modelo de criptografia simétrica

- Ataque de força bruta
  - Tentativa de obter uma chave que realize uma tradução inteligível do texto cifrado

Tamanho da chave (bits)	**Chaves possíveis**	**Tempo para realizar 10^6 decriptografias/µs**
32	$2^{32} = 4{,}3 \times 10^9$	2,15 milissegundos
56 (Ex.: DES)	$2^{56} = 7{,}2 \times 10^{16}$	10,01 horas
128 (Ex.: AES)	$2^{128} = 3{,}4 \times 10^{38}$	$5{,}4 \times 10^{18}$ anos
168 (Ex.: 3DES)	$2^{168} = 3{,}7 \times 10^{50}$	$5{,}9 \times 10^{30}$ anos

Tabela com tempo médio exigido para busca completa da chave

TIPOS DE ALGORITMOS DE CROPTOGRAFIA SIMETRICA

DES – Data Encryption Standard

- Autor: IBM, janeiro de 1977
- Chave: 56 bits
- Comentário: Muito fraco para uso atual.

Triple DES

- Autor: IBM, início de 1979.
- Chave: 168 bits
- Comentário: **Muito antiga e fraco desempenho**.

Substituições comerciais do DES

- Em resposta ao **tamanho da chave** e aos **problemas de desempenho** relacionados ao **Triple DES**, criptógrafos e empresas comerciais desenvolveram **novas cifras de bloco**.

Substituições comerciais do DES

- Blowfish (Counterpane Systems)
- RC2 (RSA)
- RC4 (RSA)
- IDEA (Ascon)
- Cast (Entrust)
- Safer (Cylink)
- RC5 (RSA)

Substituições comerciais do DES

- Pode-se **escolher um tamanho de chave que seja suficientemente grande** para tornar o seu algoritmo criptográfico imune a um **ataque de força bruta sobre a chave**, ou ao menos **tornar o ataque de força bruta impraticável**.

Blowfish

- Autor: Bruce Schneier
- Chave: 1 a 448 bits
- Comentário: Velho e lento.

RC2

- Autor: Ronald Rivest, RSA Data Security
  Meado dos anos 80.
- Chave: 1 a 2048 bits
- Comentário: quebrado em 1996.

RC4

- Autor: **Ronald Rivest,**
  RSA Data Security, 1987

- Chave: 1 a 2048 bits

- Comentário: **Algumas chaves são fracas**.

IDEA – International Data Encryption Algorithm

- Autor: **Massey & Xuejia, 1990**.
- Chave: 128 bits
- Comentário: **Bom, mas patenteado**.
- Usado no PGP (Pretty Good Privacy).
  https://www.openpgp.org/about/

RC5

- Autor: Ronald Rivest,
  RSA Data Security, 1994.
- Chave: 128 a 256 bits
- Comentário: **Bom, mas patenteado**.

Twofish

- Autor: Bruce Schneier, 1997
- Chave: 128 a 256 bits
- Comentário: **Muito forte, amplamente utilizado**.

Serpent

- Autor: Anderson, Biham, Knudsen
  1997
- Chave: 128 a 256 bits
- Comentário: **Muito forte**.

Rijndael (Origem do AES)

- Janeiro de 1997,

- **NIST** (**National Institute of Standards and Technology**), encarregado de aprovar padrões para o governo federal dos EUA, patrocinou um **concurso** para um **novo padrão criptográfico para uso não-confidencial**.

Rijndael

- A ser chamado **AES** (**Advanced Encrytion Standard**)

- Regras do concurso:
  - O algoritmo deveria ser uma cifra de bloco simétrica.
  - Todo o projeto deveria ser público.
  - Tamanho de chaves: 128, 192, 256 bits
  - Implementado, possivelmente, em SW e HW.
  - O algoritmo deveria ser público ou licenciado em termos não-discriminatórios.

Rijndael

- **15 propostas**, **conferências públicas**, **análises criptográficas** para encontrar falhas.

- **Agosto de 1998** foram selecionados 5 propostas finalistas.

Rijndael

- **Ultima votação**:
  - **Rijndael** (Daemen, Rijmen) – **86 votos**
  - Serpent (Anderson, Biham, Knudsen) – 59 votos
  - Twofish (Bruce Schneier) – 31 votos
  - RC6 (RSA) – 23 votos
  - MARS (IBM) – 13 votos

Rijndael

- Autor: Daemen & Rijmen
- Chave: 128 a 256 bits
- **Novembro de 2001**, o Rijndael **se tornou o padrão do governo dos EUA**, publicado como o Federal Information Processing Standard (FIPS 197).
- Comentário: **Melhor escolha**.

Rijndael

- O algoritmo foi projetado não só por **segurança**, mas também para **aumentar a velocidade**.

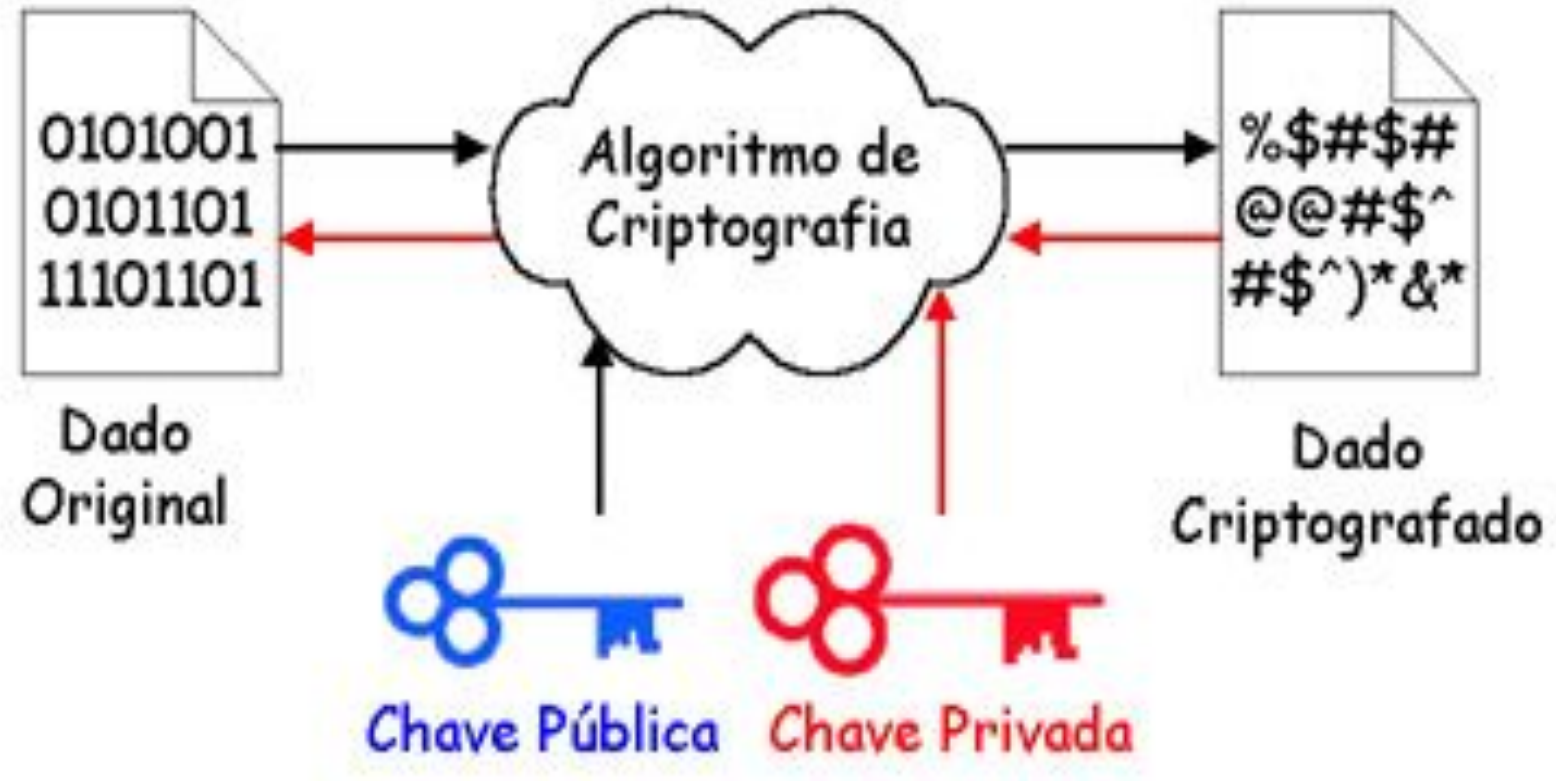
- Uma **boa implementação de software** em uma máquina de **2 GHz** deve ser capaz de alcançar uma **taxa de criptografia** de **700 Mbps,** que é rápida o suficiente para codificar **mais de 100 vídeos MPEG-2** em tempo real.

AES (novo nome para o Rijndael)

- **A**dvanced **E**ncryption **S**tandard
- **Tamanho do Bloco**: 128 bits
- **Comprimento da Chave**: **128**, 192, **256, 512** bits.

Criptografia Assimétrica (chaves públicas)

Criptografia Assimétrica



Criptografia Assimétrica

- Segundo Stallings, a criptografia assimétrica (chaves públicas) representa a maior revolução na história da criptografia

- A criptografia de chaves públicas oferece uma mudança radical em relação a tudo o que havia sido feito

- Algoritmos baseados em funções matemáticas e não em substituição e transposição.

- Grande parte da teoria dos criptosistemas de chave pública baseia-se na teoria dos números.

Criptosistemas de chave pública

- O conceito de criptografia de chave pública evoluiu da tentativa de atacar dois dos problemas mais difíceis associados à criptografia simétrica:
  - Distribuição de chaves
    - Compartilhamento de chaves
  - Assinaturas digitais
    - Mecanismo de assinaturas de documentos eletrônicos semelhantes ao mecanismo dos documentos em papel

Criptosistemas de chave pública

- Os algoritmos assimétricos contam com uma chave para criptografia e uma chave diferente, porém relacionada, para decriptografia
- Esses algoritmos possuem as seguintes características:
  - É computacionalmente inviável determinar a chave de decriptografia conhecendo-se o algoritmo e a chave de criptografia
  - As chaves relacionadas tanto podem ser usadas para criptografia e decriptografia (Ex.: RSA)

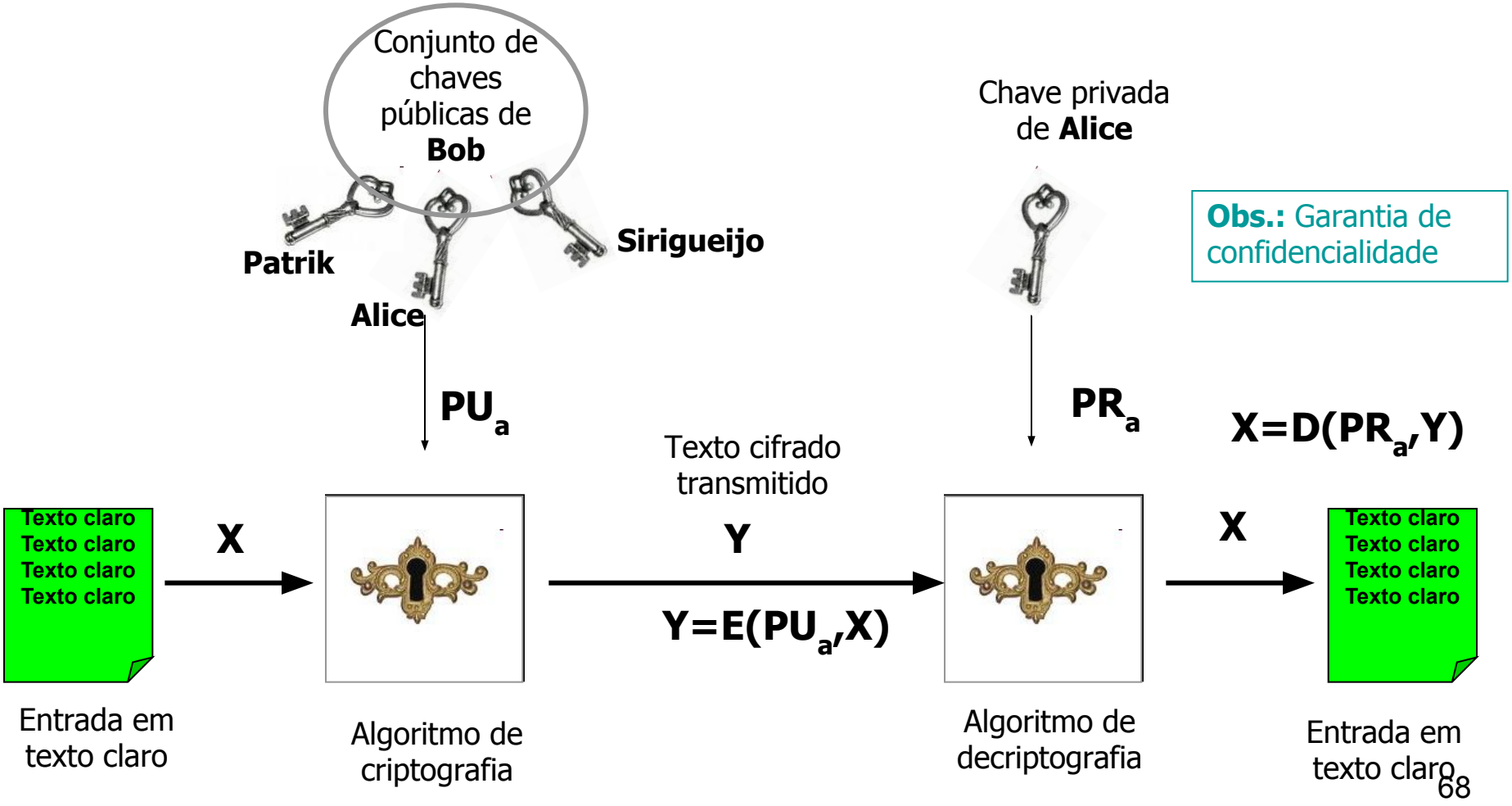
Criptosistemas de chave pública

- Um esquema de criptografia de chave pública possui os seguintes elementos:
  - Texto claro
  - Algoritmo de criptografia
  - Chaves pública e privada
  - Texto cifrado
  - Algoritmo de decriptografia

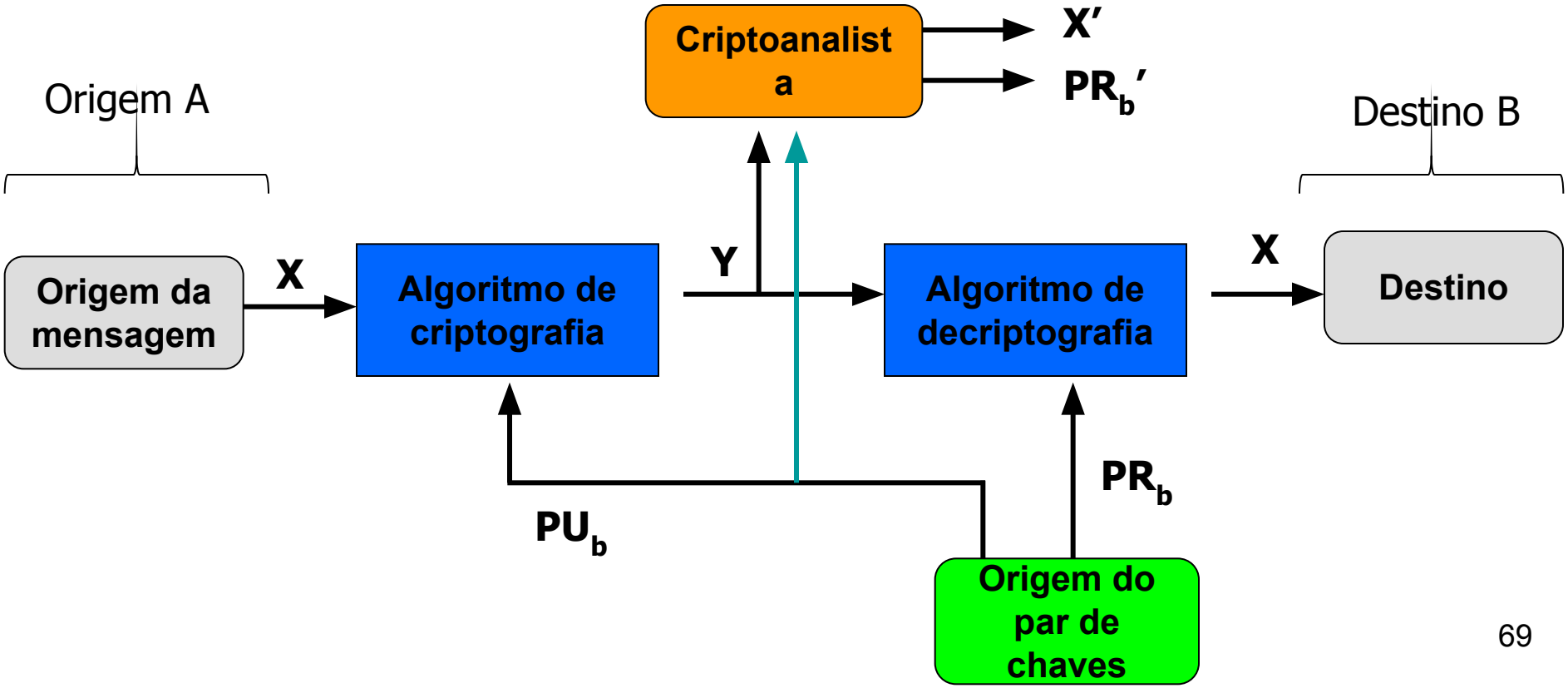
Criptosistemas de chave pública

- Etapas essenciais para o uso da criptografia de chaves públicas
  - 1 – Cada usuário gera um par de chaves para criptografar/decriptografar mensagens
  - 2 – Cada usuário coloca sua chave pública em algum registro público ou local acessível
  - 3 – Se **Bob** deseja enviar uma mensagem confidencial para **Alice** , Bob criptografa a mensagem usando a chave pública de Alice
  - 4 – Quando Alice recebe a mensagem, ela decriptografa usando sua chave privada

Criptosistemas de chave pública



Modelo de criptosistema de chave pública



O Problema da Distribuição de Chaves

Criptografia de Chave Pública

- Na **criptografia simétrica**, a mesma chave é usada para encriptar e decriptar.

- Na **criptografia assimétrica** a chave utilizada para encriptar não é usada para decriptar.

- As chaves são significativamente diferentes: **(K_e, K_d)**

Criptografia de Chave Pública

- O relacionamento é matemático; o que uma chave encripta a outra decripta:

$$\mathbf{C = E(k_e, P)} \qquad \mathbf{D(K_d, C) = P}$$

Um exemplo de chave pública

p:fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b

91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

q: 962eddcc369cba8ebb260ee6b6a126d9346e38c5

g:678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b

71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

y:2dbebe746b73439bfc8148f220984286e1856353515bebb1d55e13412644e993c75926

dca2afdf731c1aa8f944876b86a679d256f2fa4c983a1135c7d76e6390

Um exemplo de chave privada

p:fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b

91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

q: 962eddcc369cba8ebb260ee6b6a126d9346e38c5

g:678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b

71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

x:5445fb6a341e4ae1182ef22ac7c0ff8c9f3a69e2

Criptografia de Chave Pública

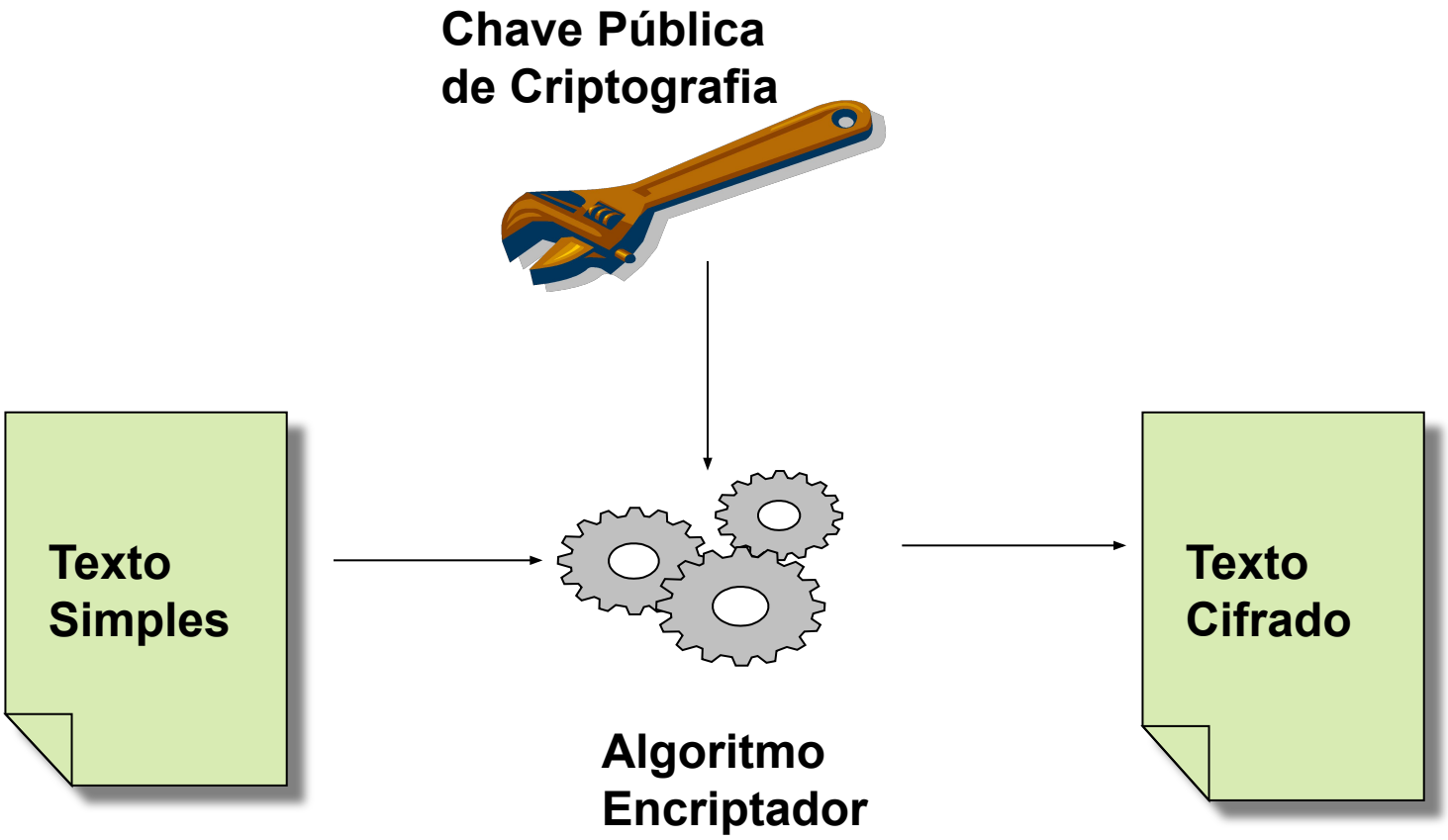
- É possível criar uma **algoritmo criptográfico** no qual **uma chave encripta** ($\mathbf{K_e}$) e uma **outra decripta** ($\mathbf{K_d}$):

$$\mathbf{D(\ K_d,\ E(k_e,\ P)\ ) = P}$$

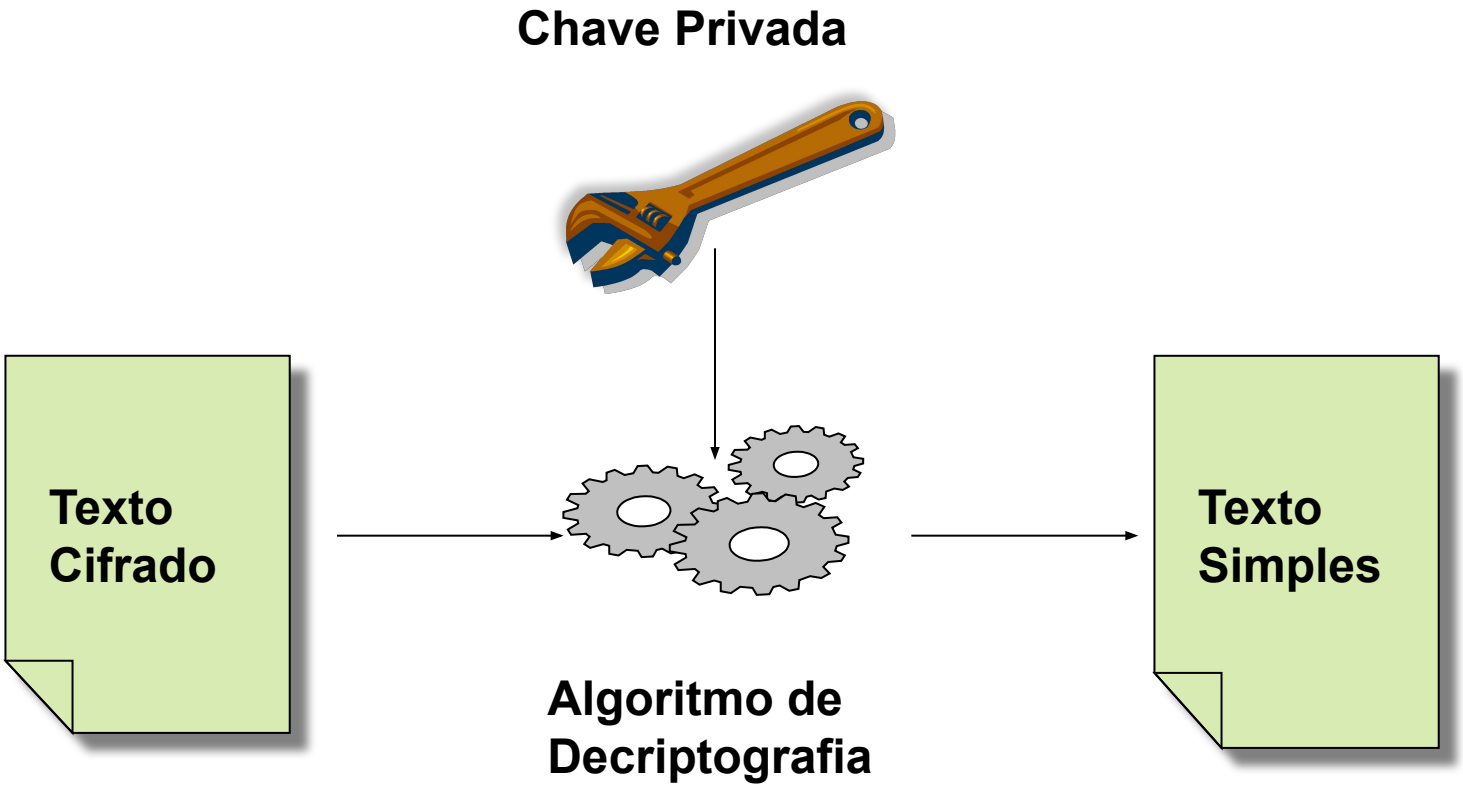
Criptografia de Chave Pública

- Porque ambas as chaves são necessárias para cifrar e decifrar a informação, **uma delas pode se tornar pública** sem pôr a segurança em perigo.
- Essa chave é conhecida como **chave pública** ($\mathbf{K_e}$).
- E sua contraparte é chamada **chave privada** ($\mathbf{K_d}$).

Criptografando com Chave Pública



Decriptografando com Chave Privada



Gerenciamento de chaves públicas

- Problema:

  Se **Alice e Bob não se conhecem um ao outro**, como eles irão **obter as respectivas chaves públicas** para iniciar a comunicação entre eles ?

- Como Alice (Bob) pode ter certeza que está realmente obtendo a chave pública de Bob (Alice) ?

Gerenciamento de chaves públicas

- A solução óbvia: **Bob coloca sua chave pública na sua página Web.**
- Não funciona !!!
- Suponha que Alice queira se comunicar com Bob.

Gerenciamento de chaves públicas

- Alice, então, precisa pesquisar a chave pública de Bob na página dele.
- Como ela fará isso?
- Alice começa por digitar a URL de Bob, em seu navegador.

Gerenciamento de chaves públicas

- O navegador pesquisa o endereço DNS da página de Bob e envia ao site Web de Bob, uma solicitação HTTP-GET.

- Infelizmente, suponha que **Trudy** intercepta a solicitação GET e **responde a Alice com uma página falsa**, fazendo a substituição da chave pública de Bob pela chave pública dela.

Gerenciamento de chaves públicas

- Quando Alice envia sua primeira mensagem criptografada, será com E_T (a chave pública de Trudy).
  - Necessário um mecanismo apropriado para que se possa disponibilizar chaves.
    - Servidor **on-line** na Internet ?

Gerenciamento de chaves públicas

- Dois problemas:
  - **Escalabilidade**
  - **Falha do servidor**

Gerenciamento de chaves públicas

- Uma Solução para escalabilidade e disponibilidade:
  - **Replicação de servidores**

Gerenciamento de chaves públicas

- Outra solução:

  Uma **Autoridade Certificadora** !

Desempenho

- Para informação em **grande quantidade**, **Algoritmos de chave pública são lentos**.
  - (20Kb a 200Kb) por segundo.
    Muito lento para processamento de dados em volume.

- **Algoritmos de chave simétrica** podem encriptar informação em **grande quantidade** bem **mais rapidamente**.

  - (10Mb, 20Mb, 50 Mb ou mais) por segundo.

Desempenho

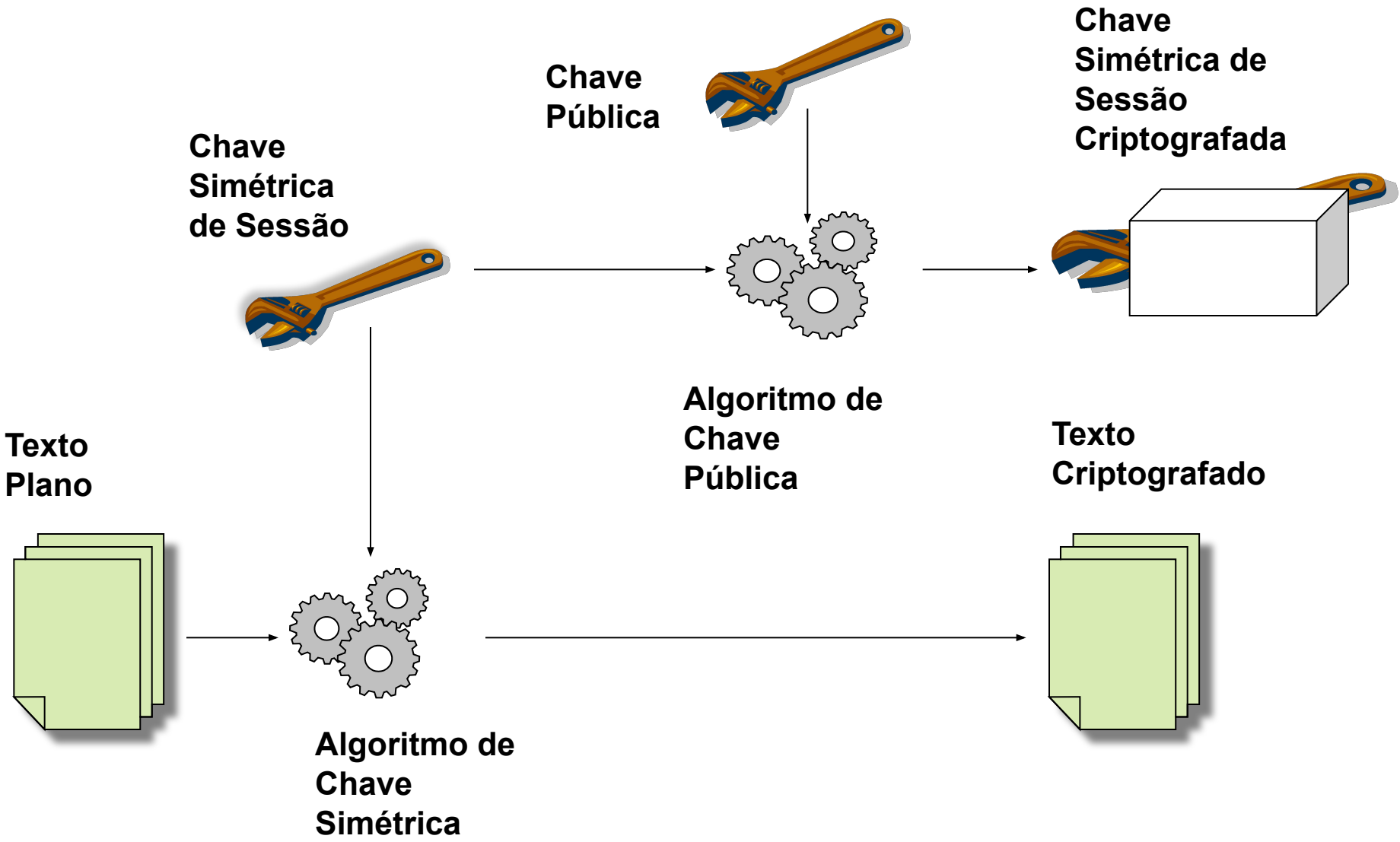
- Encriptar 128 bits (tamanho provável de uma chave simétrica), não leva tanto tempo.

- Solução: **usar a combinação de criptografia de chave simétrica e de chave pública**.

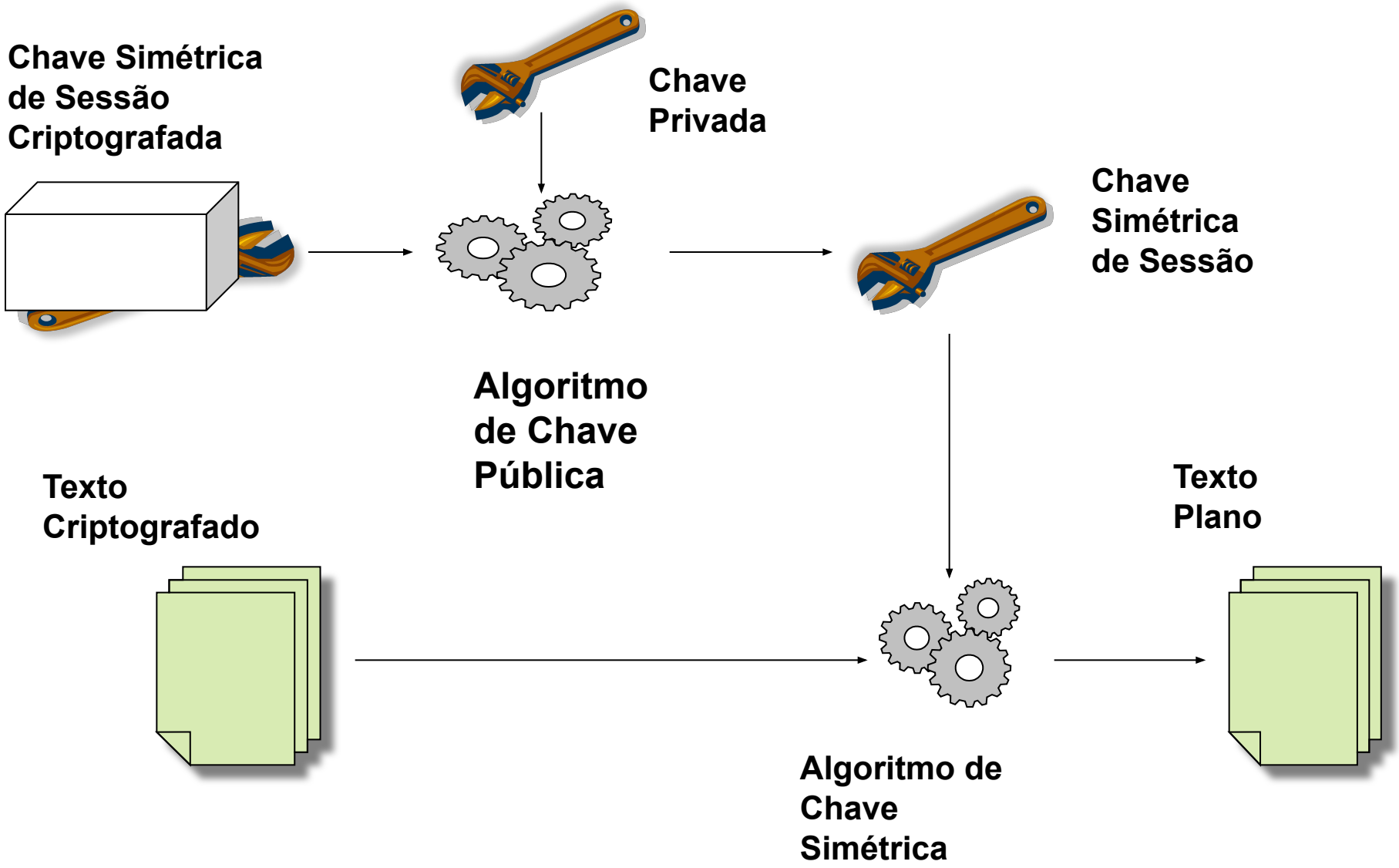
Envelope Digital

- Processo usado para **criptografar informação em grande quantidade**
  - utilizando a **criptografia de chave simétrica** e
  - **criptografando a chave simétrica de sessão** com um **algoritmo de chave pública**.

Criptografando em Envelope Digital



Descriptografando o Envelope Digital



Vantagem do Envelope Digital

- Ao invés do segredo ser compartilhado antecipadamente o segredo é compartilhado através da chave simétrica de sessão.
- A chave pública que não precisa estar protegida.

Algoritmos mais utilizados

- Três algoritmos são mais usados para resolver o **problema da distribuição de chaves**:

  - **DH** (Diffie-Hellman, 1976)
    (Stanford University)
  - **RSA** (**R**ivest, **S**hamir, **A**dleman) (M.I.T, 1978)

  - **El Gamal** (1985)

Tipos de cifragem

Cifras de fluxo vs. Cifras de bloco

- Cifras de fluxo
  - Utilizada para codificar 1 bit ou um byte por vez
- Cifras de bloco
  - Um bloco de texto claro é tratado como um todo para produzir um bloco de texto cifrado com o mesmo tamanho
  - Têm maior aplicabilidade que as cifras de fluxo

Cifra de Feistel

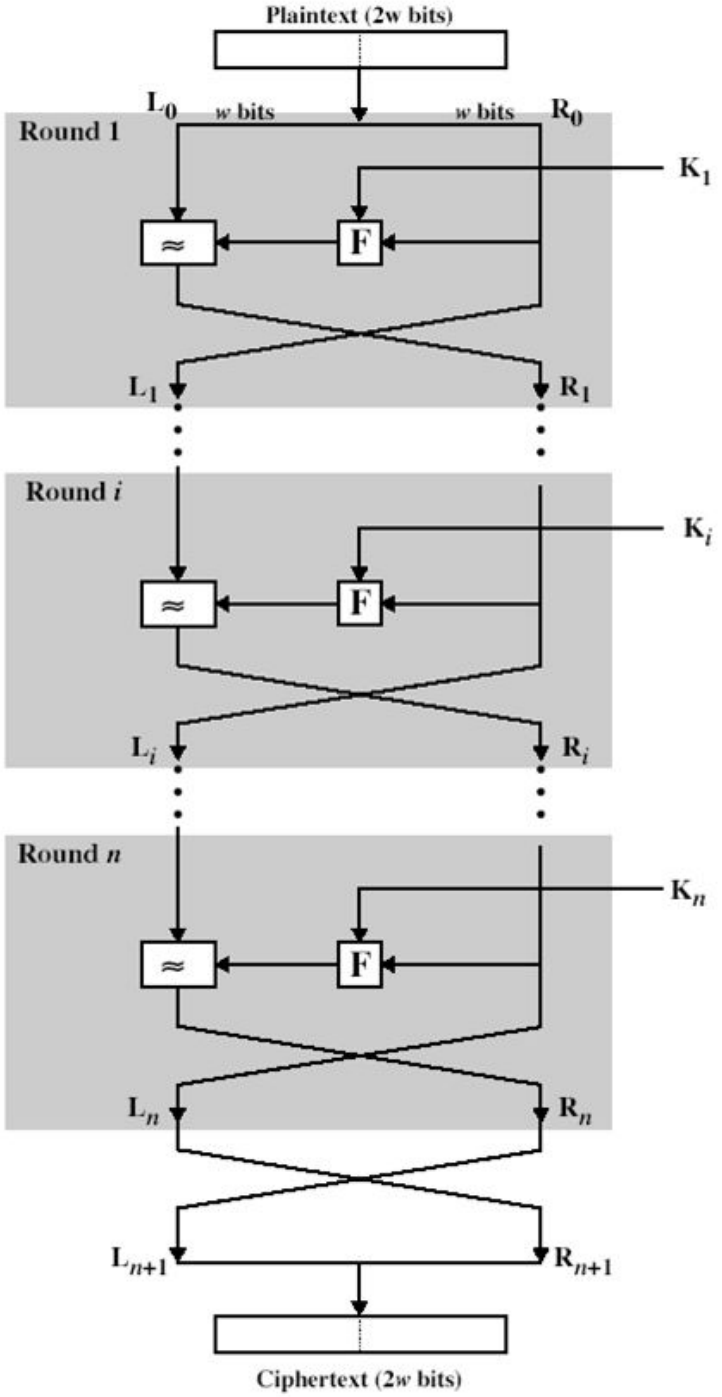
- Feistel propôs uma abordagem conhecida como cifra de produto
- Baseia-se na execução de duas ou mais cifras em sequência de tal forma que o resultado final seja criptograficamente mais forte do que qualquer uma das cifras intermediárias
- Utiliza o conceito de Difusão e Confusão para dificultar a criptoanálise estatística

Cifra de Feistel

- Parâmetros da cifra de Feistel
  - Tamanho do bloco
    - Blocos maiores significam maior segurança
    - Tradicionalmente o bloco é de 64 bits
    - Outras cifras de bloco, como o AES, utiliza bloco de 128 bits
  - Tamanho da chave
    - Chaves maiores significam maior segurança
    - 128 bits tornou-se um tamanho comum
  - Número de rodadas
    - Essência da cifra (quantidade de execuções)
    - 16 rodadas é um tamanho típico
  - Função rodada
    - Quanto maior mais seguro.

Cifra de Feistel

- L_0
  - Metade da esquerda do bloco
- R_0
  - Metade da esquerda do bloco
- K
  - Chaves e sub-chaves
- F
  - Função rodada
- ≈
  - Operação de OU exclusivo



Outras cifras de bloco

- A cifra de Feistel serviu de base para famosos algoritmos criptográficos
  - **DES** (***D**ata **E**nciptation **S**tandard*)
    - Desenvolvido na década de 1960 pela IBM com o code nome LUCIFER
    - Utiliza blocos de 64 bits e chave de 56 bits
  - **3DES** (Triplo DES)
    - Basicamente o DES executado 3 vezes em sequência
  - AES (***A**dvanced **E**ncryptation **S**tandard*)

Protocolos com Criptografia

Segurança nas Camadas

- Com exceção da **segurança na camada física**, quase **toda segurança se baseia em princípios criptográficos**.

Criptografia de Enlace

- Na camada de enlace, os quadros em uma linha ponto-a-ponto podem ser codificados, à medida que saem de uma máquina, e decodificados quando chegam em outra.

Criptografia de Enlace

- Vários detalhes de criptografia poderiam ser tratados na camada de enlace, no entanto, **essa solução se mostra ineficiente, quando existem vários switches**.
  - Necessário decriptar os pacotes nos switches, o que pode tornar esses vulneráveis a ataques.

Criptografia na Camada de Rede

- A segurança do **Protocolo IP** funciona nesta camada.
- IPSec (RFC 1825)
  - Protocolo de criptografia para tunelamento, criptografia e autenticação.
    - Dois modos:
      - Modo transporte se protege o conteúdo útil do pacote IP
      - Modo túnel se protege o pacote IP completo.

Criptografia na Camada deTransporte

- É possível criptografar conexões fim-a-fim, ou seja processo-a-processo.

- **SSL** (Security Socket Level)

- **TLS** (Transport Level Security)

Criptografia na Camada da Aplicação

- **S/MIME** (**S**ecure/**M**ultipupose **I**nternet **M**ail **E**xtensions)
- **SET** (Secure Electronic Transactions)
- **HTTPS** (HTTP sobre SSL)