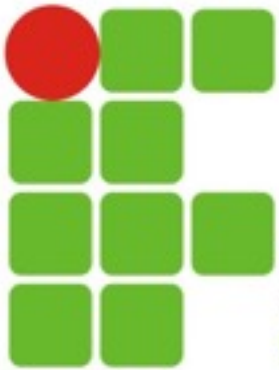


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança de Rede

Criptografia

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

- Criptografia tem origem do grego *kryptos* (oculto) e *graphein* (escrita).

- A criptografia é o estudo de técnicas para a comunicação e armazenamento seguro de dados.

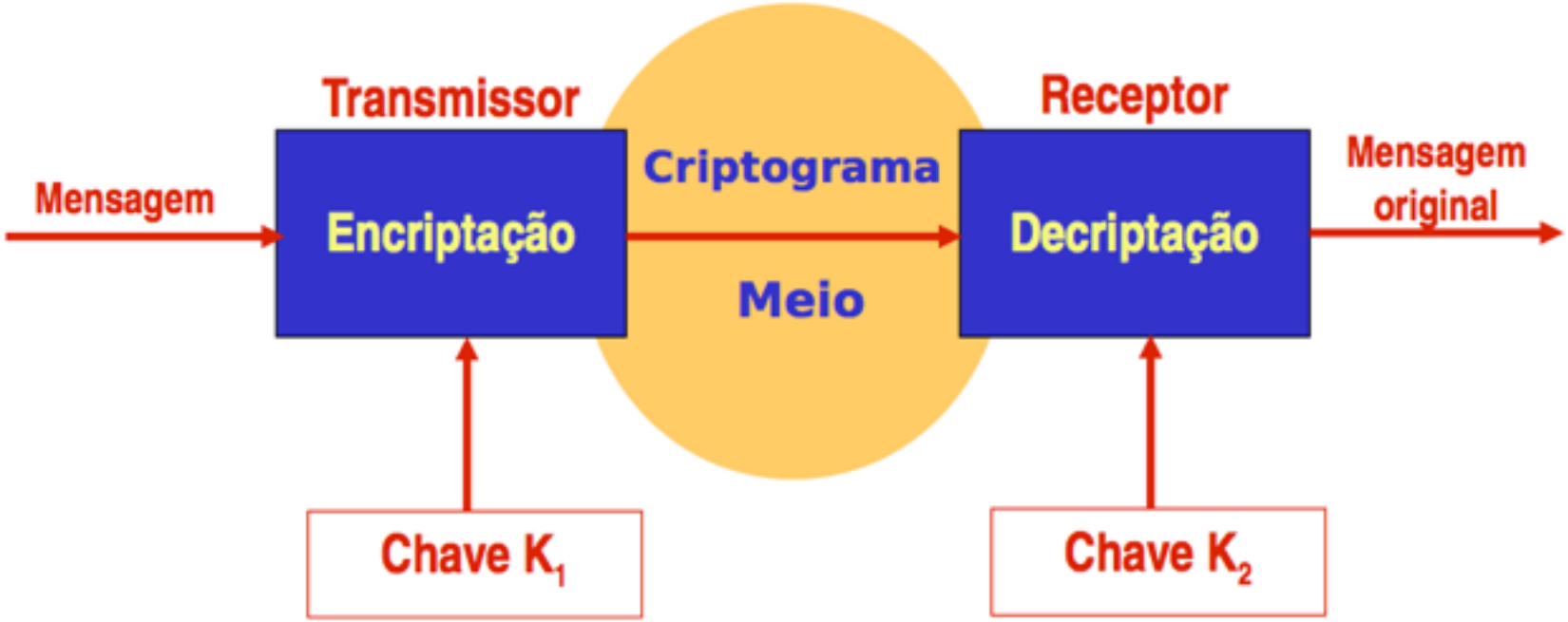
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tipos de Criptografia

- Criptografia simétrica
  - Utiliza uma única chave para encriptar e decriptar a mensagem.
- Criptografia Assimétrica
  - Cada entidade possui uma chave pública e uma chave privada.
  - Uma chave é privada e apenas o proprietário tem acesso, a outra é pública e é compartilhada com qualquer um que queira encriptar a mensagem.
- Funções de Hash
  - Não utiliza chave.
  - É usada para verificar a integridade dos dados.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução



Em Algoritmos Simétricos $K_1 = K_2 (K)$

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Modelo de criptografia simétrica

- Método de Substituição
  - O uso mais antigo conhecido da cifra de substituição, e o mais simples, foi feito pelo Imperador romano Júlio César
    - Cifra de César
      - Consiste em substituir cada letra do alfabeto pela letra que fica três posições adiante no alfabeto.

Claro:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Exemplo:

```
Claro: saida pela direita ze
Cifra: vdlgd shod gluhlwd ch
```

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Modelo de criptografia simétrica

- Substituição (Cifra de César)
  - Se for conhecido que um determinado texto cifrado é uma cifra de César, uma criptoanálise pela força bruta será facilmente realizada...
    - Como ??
      - Testando todas as chaves
    - Quantas chaves possíveis existe ?
      - Existem 25 chaves ! (k variando de 1 até 25)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Modelo de criptografia simétrica

- Método de Transposição
  - Esse método baseia-se na aplicação de algum tipo de permutação nas letras do texto claro
    - A técnica mais simples é a de rail fence (trilho)
      - O texto claro é escrito como uma sequência de diagonais e lido como uma sequência de linhas

Exemplo:

Claro: meet me after the toga party
Escrita: m e m a t r h t g p r y e t e f e t e o a a t
Cifra: mematrhtgpryetefeteoaat

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Modelo de criptografia simétrica

- Método de Transposição
  - Um esquema mais complexo é escrever a mensagem em uma matriz MxN e ler a mensagem coluna por coluna, mas permutar a ordem das colunas

Exemplo:

Chave:	**4**	**3**	**1**	**2**	**5**	**6**	**7**
Texto claro:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Cifra: ttnaaptmtsuoaodwcoixknlypetz

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

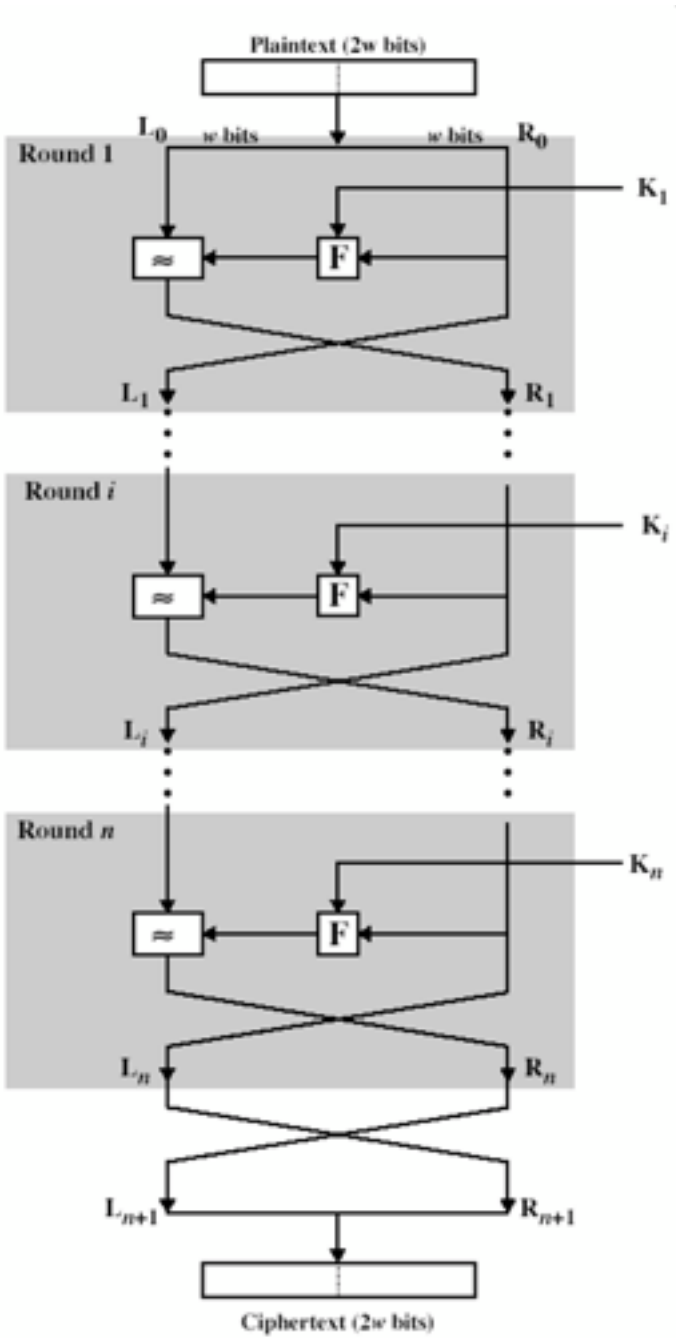
Cifra de Feistel

- 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.C

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Cifra de Feistel

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



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Outras cifras de bloco

- A cifra de Feistel serviu de base para famosos algoritmos criptográficos
  - **DES** (**D**ata **E**ncriptation **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)
    - O candidato a substituir o 3DES

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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

Modelo de criptografia assimétrica

- 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

Modelo de criptografia assimétrica

- Os algoritmos assimétricos contam com uma chave para criptografia e uma chave diferente, porem 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)

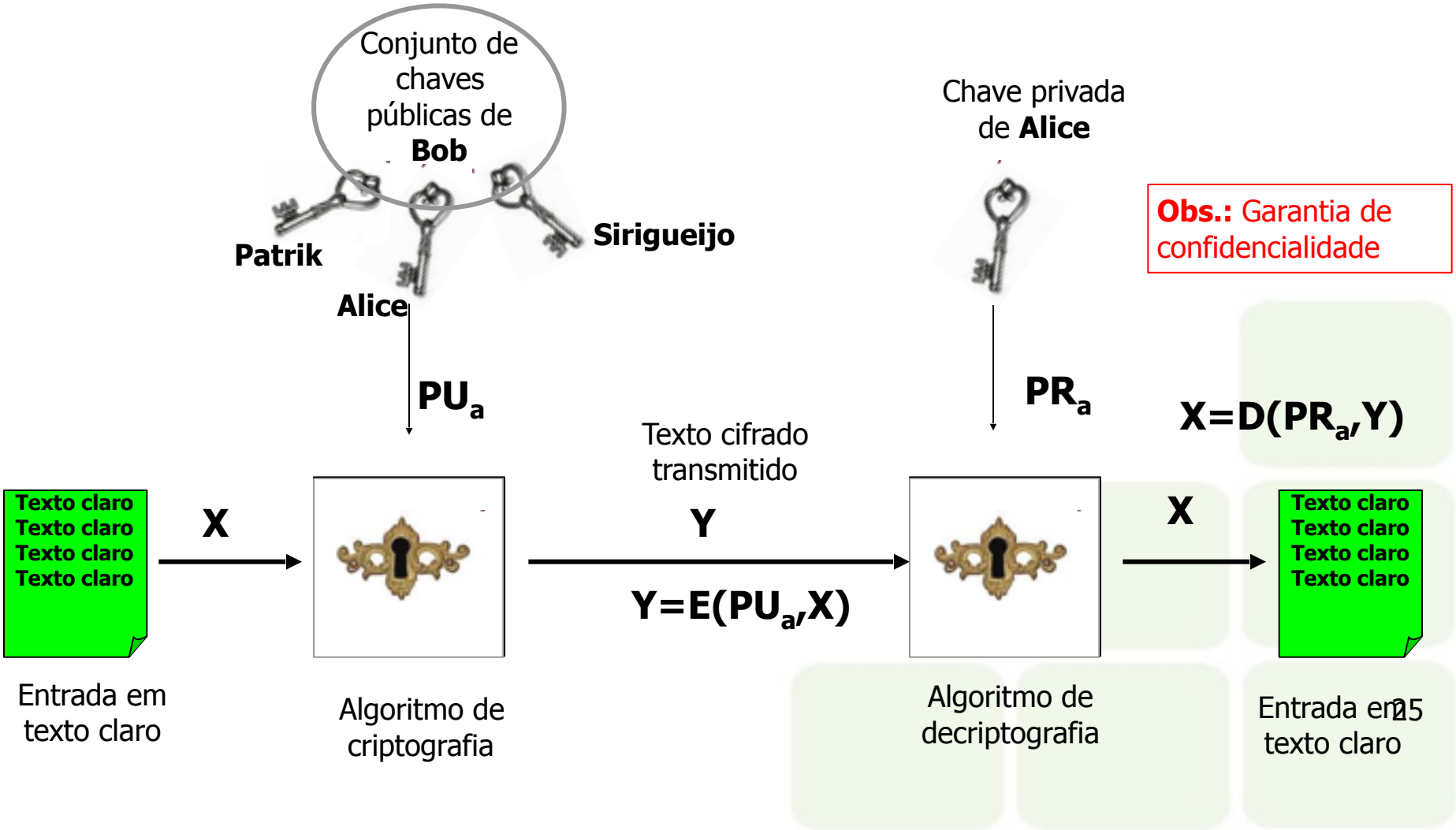
Modelo de criptografia assimétrica

- 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

Modelo de criptografia assimétrica

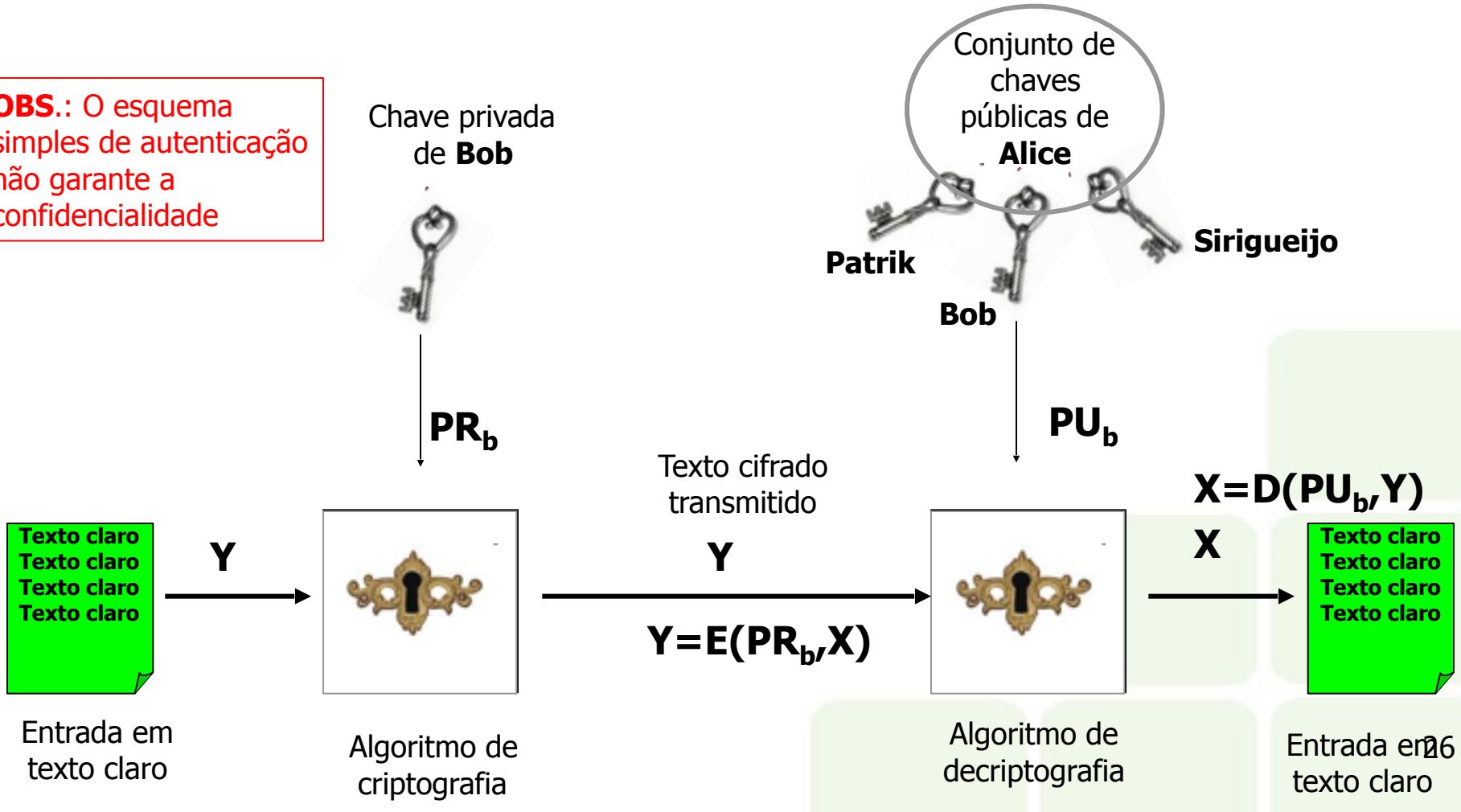
- Etapas essenciais para o uso da criptografia de chaves públicas
  - 1 – Cada usuários gera um par de chaves para criptografar/decriptografar mensagens
  - 2 – Cada usuário coloca sua chave pública em algum registro público ou local acessível
  - 3 – Se **Bob** deseja enviar uma mensagem confidencial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

Modelo de criptografia assimétrica



Modelo de criptografia assimétrica

OBS.: O esquema simples de autenticação não garante a confidencialidade



Comentários

- A criptografia de chave pública se propôs a resolver, e resolveu, dois dos maiores problemas da criptografia convencional:
  - Compartilhamento de chaves
  - Assinatura digital
- A criptoanálise em criptosistemas de chave pública também é vulnerável a ataques de força bruta
- Outro ataque é a obtenção da chave privada dada uma chave pública, visto que elas são relacionadas (até hoje esse ataque não obteve sucesso)